ID: 385171
Cookbook: browseurl.jbs
Time: 06:38:23
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

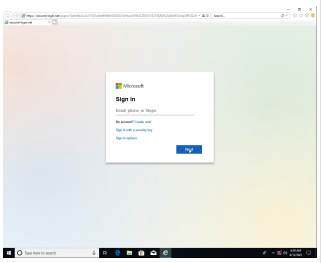
Analysis Report https://welsfargo.com-onlinebanking.co…

Overview

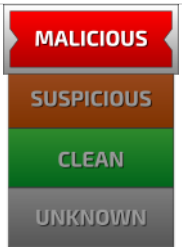
General Information

Sample URL:	https://welsfargo.com-onlinebanking.com/XTlU1aGJteE9NRk5DU0ZCUVNucGlTRkJCZD...kejA5LS1mNTY3M2RlODQzYTFhY2IwZTFjOTZiNGQ1YjI3MTU0NDk0YTgzNDVl?cid=829803269
Analysis ID:	385171
Infos:	

Most interesting Screenshot:



Detection



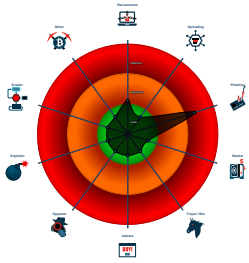
HTMLPhisher

Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish10
- Phishing site detected (based on log…
- HTML body contains low number of …
- No HTML title found

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5780 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5248 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5780 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\J87Y3MCZ.htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

- Phishing
- Compliance
- Networking
- System Summary

Click to jump to signature section

Phishing:

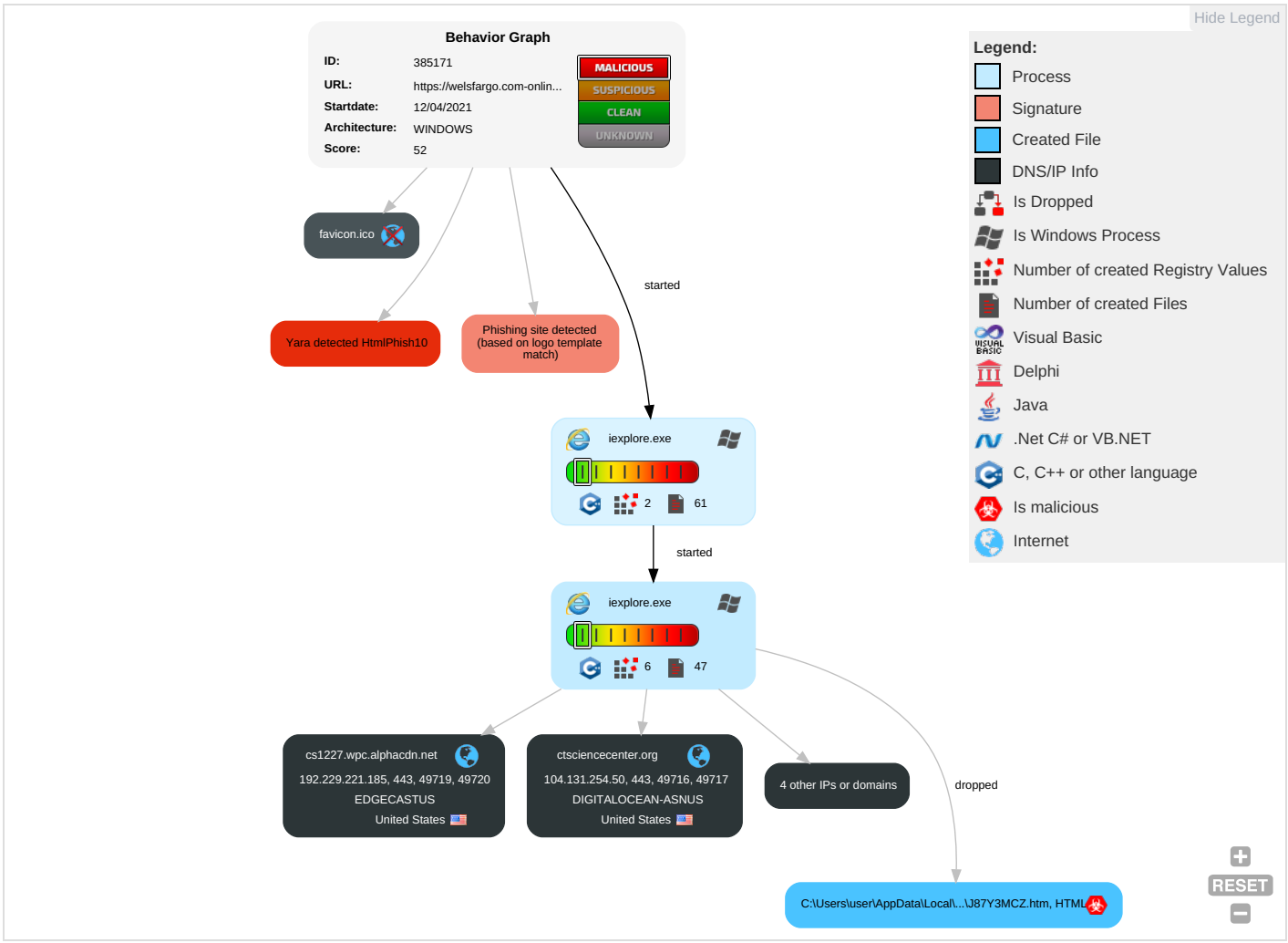
Yara detected HtmlPhish10

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

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

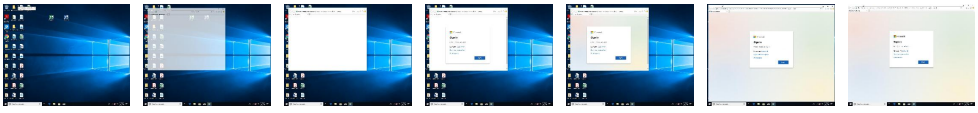
Behavior Graph

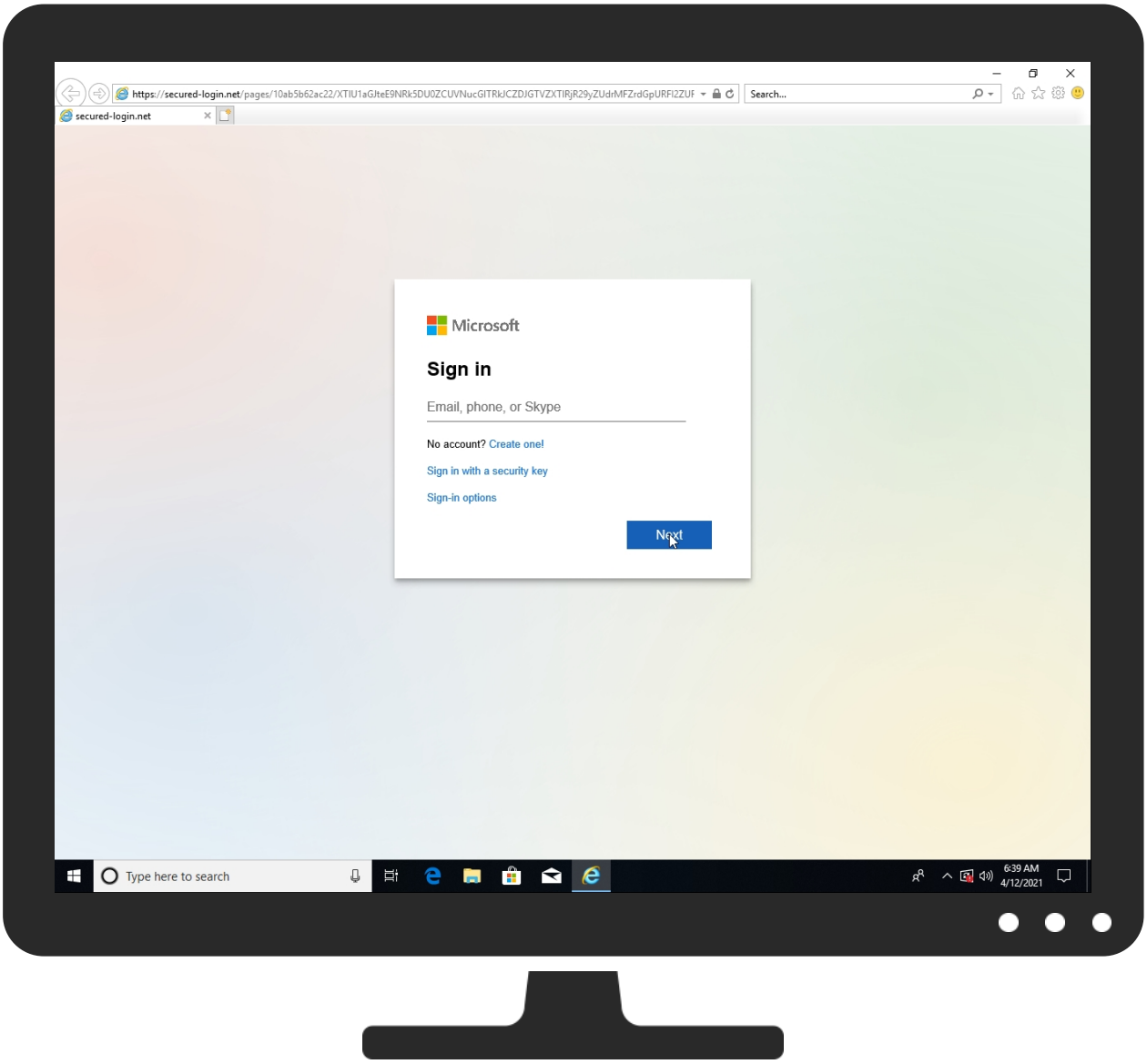


Screenshots

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://welsfargo.com-onlinebanking.com/XTlU1aGJteE9NRk5DU0ZCUVNucGlTRkJCZDJGTVZXTlRjR29yZUdrMFZrdGpURFI2ZURJMUwzbzVWV3hyY21sT1pHNXdRVVYwTkhkWmFVOVBUalpaTDBwUVZESk1abTkyZFRscE0za3lSRWt3ZEUxU1ZHWnJURzVXZFhONksySkJRVmxKVFVWVWRtMVJaekZCY2xWWVJWRTNWbE14WmpoV2QxZGxRa280VlZaUldrUjNZbWR6T1dod1dUQndSRkpJT1ZocFZ6VnJLeklwVGtKU1luZzVWMWxYY21wQ1luVjJRa28wUFMwdFZ5ODJka0pTTVdkcFFURk5hSEExVWtaTmRIWnFkejA5LS1mNTY3M2RlODQzYTFhY2IwZTFjOTZiNGQ1YjI3MTU0NDk0YTgzNDVl?cid=829803269	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cs1227.wpc.alphacdn.net	0%	Virustotal		Browse
secured-login.net	1%	Virustotal		Browse
logincdn.msauth.net	1%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
welsfargo.com-onlinebanking.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://chmln.github.io/flatpickr/examples/#flatpickr-external-elements	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://secured-login.onlinebanking.com/XTlU1aGJteE9NRk5DU0ZCUVNucGlTRkJCZDJGTVZXTlRjR29yZUdrMFZrdGp	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%	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/#intersection-observer-entry	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cs1227.wpc.alphacdn.net	192.229.221.185	true	false	• 0%, Virustotal, Browse	unknown
secured-login.net	52.22.122.101	true	false	• 1%, Virustotal, Browse	unknown
ctsciencecenter.org	104.131.254.50	true	false		high
landing.training.knowbe4.com	54.175.141.245	true	false		high
logincdn.msauth.net	unknown	unknown	false	• 1%, Virustotal, Browse	unknown
welsfargo.com-onlinebanking.com	unknown	unknown	false	• 1%, Virustotal, Browse	unknown
favicon.ico	unknown	unknown	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.ecma-international.org/news/TC45_current_work/Office%20Open%20XML%20Part%204%20-%20Marku	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://api.jqueryui.com/slide-effect/	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/moment/moment/issues/1423	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/chartjs/Chart.js/pull/4507	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://chmln.github.io/flatpickr/examples/#flatpickr-external-elements	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://stackoverflow.com/a/32954565/96342	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/madrobby/zepto/blob/master/src/zepto.js	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://stackoverflow.com/questions/30464750/chartjs-line-chart-set-background-color	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/chartjs/Chart.js/issues/5597	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://stackoverflow.com/a/26707753	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high

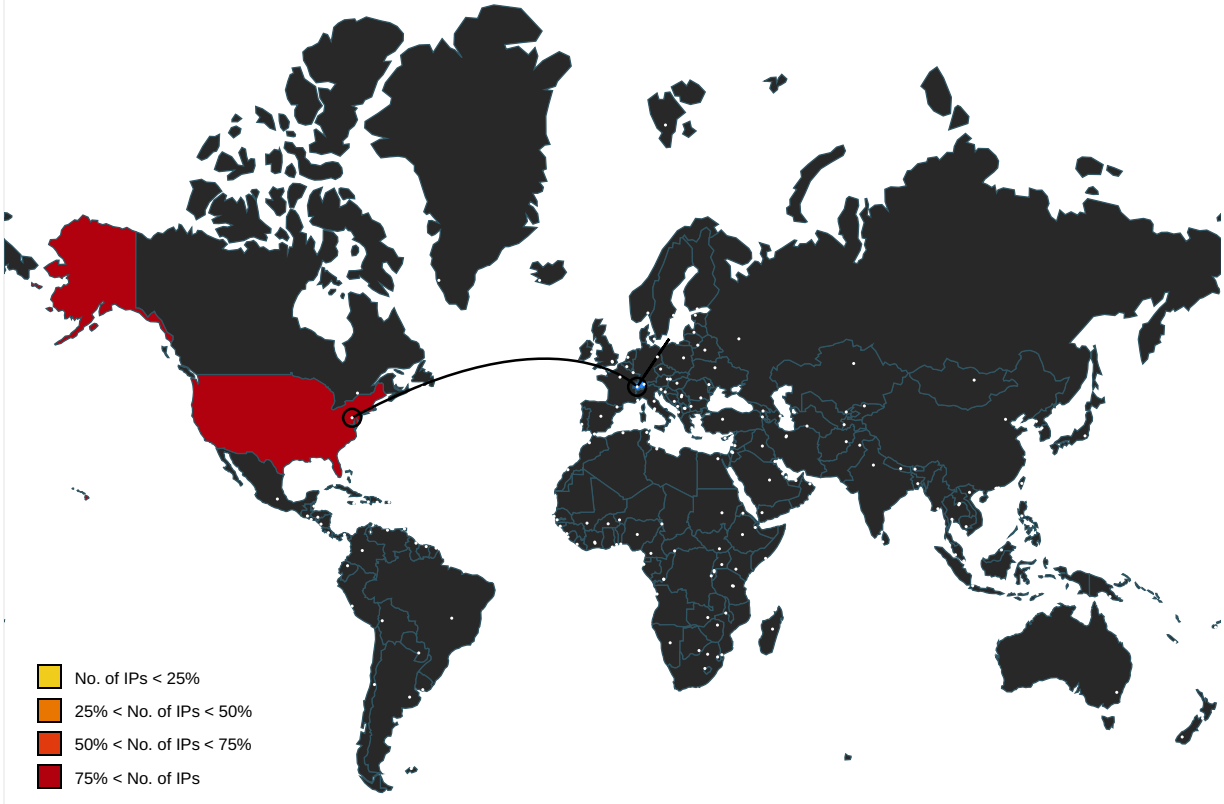
Name	Source	Malicious	Antivirus Detection	Reputation
http://jsfiddle.net/dbs4c8h0/1/	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/jquery/jquery-color	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http:// https://github.com/select2/select2/blob/master/LICENSE.md	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://api.jqueryui.com/jQuery.widget/	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://blog.jquery.com/2012/08/09/jquery-1-8-released/	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://codereview.stackexchange.com/q/13338	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://pdfmake.org	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://https://bugzilla.mozilla.org/show_bug.cgi?id=561664	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://dev.w3.org/csswg/cssom/#resolved-values	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://https://caniuse.com/download	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/chartjs/Chart.js/issues/2538	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://dev.w3.org/csswg/css-color/#hwb-to-rgb	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/jrburke/requirejs/wiki/Updating-existing-libraries#wiki-anon	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://www.apache.org/licenses/LICENSE-2.0)	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/kriskowal/es5-shim/blob/master/es5-shim.js	modernizr-79e0181ec91aff04bb01 d87cba546535ede843f75d19f5c60f 66b8dd6546971f[1].js.2.dr	false		high
http://api.jqueryui.com/button/	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://https://bugzilla.mozilla.org/show_bug.cgi?id=687787	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://https://blog.alexmaccaw.com/css-transitions	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://www.datatables.net	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/bassjobsen/Bootstrap-3-Typeahead	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://https://getbootstrap.com/docs/3.4/javascript/#transitions	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/chartjs/Chart.js/issues/4152	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://bugs.jquery.com/ticket/9917	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://api.jqueryui.com/size-effect/	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/Do/iso8601.js	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://developer.mozilla.org/en-US/docs/Web/API/EventTarget/addEventListener#Safely_detecting_optio	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://momentjs.com/guides/#/warnings/zone/	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://bugs.jquery.com/ticket/12359	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://developer.mozilla.org/en-US/docs/Web/API/EventTarget/removeEventListener	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://w3c.github.io/IntersectionObserver/#intersection-observer-interface	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://creativecommons.org/licenses/by/3.0/)	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://docs.closure-library.googlecode.com/git/closure_goog_date_date.js.source.html	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.nathanaeljones.com/blog/2013/reading-max-width-cross-browser	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bugzilla.mozilla.org/show_bug.cgi?id=649285	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://getbootstrap.com/docs/3.4/javascript/#tooltip	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/chartjs/Chart.js/issues/6104	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://jsperf.com/diacritics/18	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://api.jqueryui.com/category/ui-core/	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/twbs/bootstrap/issues/20280	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/chartjs/Chart.js/issues/4287	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://getbootstrap.com/docs/3.4/javascript/#modals	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/chartjs/Chart.js/issues/2435#issuecomment-216718158	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://jsperf.com/object-keys-vs-for-in-with-closure/3	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://stackoverflow.com/q/181348	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://getbootstrap.com/docs/3.4/javascript/#collapse	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://secured-login.onlinebanking.com/XTlU1aGJteE9NRk5DU0ZCUVNucGlTRkJCZDJGTVZXTlRjR29yZUdrMFZrdGp	{72DC8A81-9B94-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.macromedia.com/go/getflashplayer	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://www.anujgakhar.com/2014/03/01/binary-search-in-javascript/	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/chartjs/Chart.js/issues/4737	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/kkapsner/CanvasBlocker	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://www.robertpenner.com/easing/	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://w3c.github.io/IntersectionObserver/#calculate-intersection-rect-algo	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/chartjs/Chart.js/issues/3887	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://getbootstrap.com/docs/3.4/javascript/#scrollspy	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/w3c/IntersectionObserver/issues/211	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://flightschool.acylt.com/devnotes/caret-position-woes/	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://api.jqueryui.com/transfer-effect/	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/rails/jquery-ujs	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://stackoverflow.com/questions/8506881/nice-label-algorithm-for-charts-with-minimum-ticks	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://bugzilla.mozilla.org/show_bug.cgi?id=491668	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/marcj/css-element-queries	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://www.robertpenner.com/easing)	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://momentjs.com/guides/#/warnings/min-max/	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://npms.io/search?q=ponyfill.	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/chartjs/Chart.js/issues/4102	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://stackoverflow.com/q/3922139	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://api.jqueryui.com/drop-effect/	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://datatables.net/license	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://jsperf.com/getall-vs-sizzle/2	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://getbootstrap.com/docs/3.4/javascript/#buttons	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/jquery/jquery/pull/557)	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://www.html5canvastutorials.com/advanced/html5-canvas-mouse-coordinates/	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://api.jqueryui.com/menu/	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://getbootstrap.com/docs/3.4/javascript/#alerts	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/chartjs/Chart.js/issues/5208	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high
http://api.jqueryui.com/category/effects-core/	application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[1].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://bugs.jquery.com/ticket/8235	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http:// https://chartjs.gitbooks.io/proposals/content/Platform.html	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://api.jqueryui.com/dialog/	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://https://w3c.github.io/IntersectionObserver/#intersection-observer-entry	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://api.jqueryui.com/shake-effect/	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/Microsoft/tslib/blob/v1.6.0/tslib.js	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://https://stackoverflow.com/questions/10149963/adding-event-listener-cross-browser	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/imulus/retinajs/issues/8	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://jsperf.com/1-vs-infinity	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/cujojs/when/issues/410	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://https://getbootstrap.com/)	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://https://github.com/ankane/chartkick.js	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high
http://https://modernizr.com/)	application-90929fee9f5daac0ec a637129a780171565a15cebe060e2d 86c95ffac685fd7b[1].js.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.131.254.50	ctsciencecenter.org	United States		14061	DIGITALOCEAN-ASNUS	false
54.175.141.245	landing.training.knowbe4.com	United States		14618	AMAZON-AESUS	false
192.229.221.185	cs1227.wpc.alphacdn.net	United States		15133	EDGECASTUS	false
52.22.122.101	secured-login.net	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385171
Start date:	12.04.2021
Start time:	06:38:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://welsfargo.com-onlinebanking.com/XTlU1aGJteE9NRk5DU0ZCUVNucGlTRkJCZDJGTVZXTlRjR29yZUdrMFZrdGpURFI2ZURJMUwzbzVWV3hyY21sT1pHNXdRVVYwTkhkWmFVOVBUalpaTDBwUVZESk1abTkyZFRscE0za3lSRWt3ZEUxU1ZHWnJURzVXZFhONksySkJRVmxKVFVWVWRtMVJaekZCY2xWWVJWRTNWbE14WmpoV2QxZGxRa280VlZaUldrUjNZbWR6T1dod1dUQndSRkpJT1ZocFZ6VnJLeklwVGtKU1luZzVWMWxYY21wQ1luVjJRa28wUFMwdFZ5ODJka0pTTVdkcFFURk5hSEExVWtaTmRIWnFkejA5LS1mNTY3M2RlODQzYTFhY2lwZTFjOTZiNGQ1YjI3MTU0NDk0YTgzNDVl?cid=829803269
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:	7
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal52.phis.win@3/15@5/4
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, audiodg.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 204.79.197.200, 13.107.21.200, 13.88.21.125, 88.221.62.148, 104.43.193.48, 20.50.102.62 • Excluded domains from analysis (whitelisted): www.bing.com, arc.msn.com.nsatc.net, dual-a-0001.a-msedge.net, lgincdnvzeuno.ec.azureedge.net, skypedataprdcolcus16.cloudapp.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, lgincdnvzeuno.azureedge.net, e11290.dspg.akamaiedge.net, go.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, lgincdn.trafficmanager.net, blobcollector.events.data.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, go.microsoft.com.edgekey.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, skypedataprdcolwus15.cloudapp.net

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\7XIC6Q2O\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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\7XIC6Q2O\secured-login[1].xml	
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.{72DC8A7F-9B94-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33368
Entropy (8bit):	1.8811120288972754
Encrypted:	false
SSDEEP:	96:rPZAZK2NW4+NHt4+NQf4+NwNM4+yF4+g94+gOf4+gDMr4+6:rPZAZK2NWVHtVQfVwNM6F494Of4DMrS
MD5:	637A409A933B6C24F67CAC151CBAD607
SHA1:	257AD5F47581F5A1A6D606EB7459EACB3F766AEE
SHA-256:	FA0FFCC3187F1EAD2E508DE15F3D98EB40FCFD91BF16A02F05A6646867DCC203
SHA-512:	2313687F57B3788C40A8D1A6846EA7155597A7D5E5A8843418394BA45F26D75561E72B54D204992FC37E5327D17E748D106A8B6BF0F301C5CD1FDA2A54763089
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\{72DC8A81-9B94-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	38698
Entropy (8bit):	2.669013176048952
Encrypted:	false
SSDEEP:	192:r9ZmQS64kCjJ2dWeMRa02bgf/QYbgDubgZbgI8bgxbgvbgKbgpbgrbgsbg6g:rTz9F8Y03Rb2iQYzo/8c6vke5G
MD5:	3707FA64B763B322216771E2853779A8
SHA1:	6E4D06DC1BCE1476170ECF2C257CF68F027C58BB
SHA-256:	54010F5E147129E1071A68E46FA9084B16CC190EEEF65178F5F8F528477F514D
SHA-512:	429244781CA275FB6C630300609468552A9A366C1AFFA4FF8ADB921D7261EC7BB4AD1754F1DA49DD4CB6DD049DE4CE5B797CBBE5EFB9DBB046099929F72BAC77
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\{797E165A-9B94-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.56594732250189
Encrypted:	false
SSDEEP:	48:IwPGcpriGwpagG4pQ8hGrapbSPGQpKtWG7HpRnTGIpG:rFZKQA68xBSZAtBTVA
MD5:	DF74F24EF82A2522870467E5388B8192
SHA1:	AAA822FBD51C29E465B95C75FE132FD260BA2A6D
SHA-256:	311A0771BD1AE8FB05637D35B1F5FAD76616539604DB7EF202F6F96729CAB184
SHA-512:	D8D766E741E6A9BD16C5302F02D628F748094D4BE95EA1684F4A5A8EAB51C9D6349D7A867BB90AE51BA589437258C1203C4B07D315DCAC01EF89E391335D604
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{797E165A-9B94-11EB-90E4-ECF4BB862DED}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

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 C
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\MEEXW4H4\2_bc3d32a696895f78c19df6c717586a5d[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1864
Entropy (8bit):	5.222032823730197
Encrypted:	false
SSDEEP:	48:yvswNIBLBpJawmMH44log6gw/MHm7pJroog6gwkMH9Xog6gwdMHdqdyqog7C:ykfXYx+odPcs9B
MD5:	BC3D32A696895F78C19DF6C717586A5D
SHA1:	9191CB156A30A3ED79C44C0A16C95159E8FF689D
SHA-256:	0E88B6FCBB8591EDFD28184FA70A04B6DD3AF8A14367C628EDD7CABA32E58C68
SHA-512:	8D4F38907F3423A86D90575772B292680F7970527D2090FC005F9B096CC81D3F279D59AD76EAFCA30C3D4BBAF2276BBAA753E2A46A149424CF6F1C319DED5A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://logincdn.msauth.net/shared/1.0/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6z" fill="url(#A)"/><path d="M394.2 1815.6c746.58 0 1351.8-493.2 1351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 1815.6 394.2 1815.6z" fill="url(#B)"/><path d="M1548.6 1885.2c631.92 0 1144.2-417.45 1144.2-932.4S2180.52 20.4 1548.6 20.4 404.4 437.85 404.4 952.8s512.276 932.4 1144.2 932.4z" fill="url(#C)"/><path d="M265.8 1215.6c690.246 0 1249.8-455.595 1249.8-1017.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUnits="userSpaceOnUse" gradientTransform="translate(1466.4 393.6) rotate(90) scale(1401.6 1720.8)"><stop stop-color="#107c10"/><stop offset="1" stop-color="#c4c4c4" stop-opacity="0"/></radialGradient><r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\J87Y3MCZ.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	8554
Entropy (8bit):	5.652272148631601
Encrypted:	false
SSDEEP:	96:O4/A7CuP7Og5/FLyeA3/AtG3O/6mSFtO3DUnfZKSFCAd73O/ZuujFtOrIPkP9NeV:OHPL5/AVOQnOzW5O7nOv2Qgw2lyBc
MD5:	0C5787917D3BBD0EB3C22A8457F5E045
SHA1:	479FE22C82B6CB126E27C0681CEFEDC88DD6DE4F
SHA-256:	48670236D2BFCB1A0D7B722592EDEFC055AB1BDCCC99ABDF252EDCF98921EA3F
SHA-512:	4C4E7707A4F531813F526E53C5938E80A6B5E7961028999AEEE0A4B2AFEF7383792F2B23698725793527F9B56DD16D3ED5ECBE31F6E4406C207EA2FE35663957
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\J87Y3MCZ.htm, Author: Joe Security

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\J87Y3MCZ.htm	
Reputation:	low
IE Cache URL:	http://https://secured-login.net/pages/10ab5b62ac22/XTlU1aGJteE9NRk5DU0ZCUVNucGlTRkJCZDJGTVZXTlRjR29yZUdrMFZrdGpURFI2ZURJMUwzbzVWV3hyY21sT1pHNXdRVVYwTkhkWmFVOVBUalpaTDBwUVZESk1abTkyZFRscE0za3lSRWt3ZEUxU1ZHWnJURzVXZFhONksySkJRVmxKVFVWVWRtMVJaekZCY2xWWVJWRTNWbE14WmpoV2QxZGxRa280VlZaUldrUjNZbWR6T1dod1dUQndSRkpJT1ZocFZ6VnJLekIwVGtKU1luZzVWMWxYY21wQ1luVjJRa28wUFMwdFZ5ODJka0pTTVdkcFFURk5hSEExVWtaTmRIWnFkejA5LS1mNTY3M2RlODQzYTFhY2IwZTFjOTZiNGQ1YjI3MTU0NDk0YTgzNDVl
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\PSUEOSZZ\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
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\WJ8I2OL4\F0EPYP4W.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	557
Entropy (8bit):	5.7510763426202445
Encrypted:	false
SSDEEP:	12:3R+xn/Qfkqb0DXbGUDHGG05HDUr2+KigatEZxhW+j8I4C/4AEdeIQL:3EIfRb4vl5K23irtgW+AnC/NEkj
MD5:	445A799C5E8E7A34617B3955187F4483
SHA1:	FEC9BB8AE4028F8AC3F911BB59F84DA096D556C1
SHA-256:	A936B7C39E680DE8CFD7E8D522CE3C62AD4F823CCB6147D206BCAEC26A8FE5FC
SHA-512:	7FB17CB74CE72647405A63A6E0D8CDDE0FB64680FAE49C8C381A149AF41D3553258BD21BB336EE685F8ECFA3C1069B1923BF4A36CB8E7C01FD09E06D6E60728
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://welsfargo.com-onlinebanking.com/XTlU1aGJteE9NRk5DU0ZCUVNucGlTRkJCZDJGTVZXTlRjR29yZUdrMFZrdGpURFI2ZURJMUwzbzVWV3hyY21sT1pHNXdRVVYwTkhkWmFVOVBUalpaTDBwUVZESk1abTkyZFRscE0za3lSRWt3ZEUxU1ZHWnJURzVXZFhONksySkJRVmxKVFVWVWRtMVJaekZCY2xWWVJWRTNWbE14WmpoV2QxZGxRa280VlZaUldrUjNZbWR6T1dod1dUQndSRkpJT1ZocFZ6VnJLekIwVGtKU1luZzVWMWxYY21wQ1luVjJRa28wUFMwdFZ5ODJka0pTTVdkcFFURk5hSEExVWtaTmRIWnFkejA5LS1mNTY3M2RlODQzYTFhY2IwZTFjOTZiNGQ1YjI3MTU0NDk0YTgzNDVl?cid=829803269
Preview:	<html>. <head>. <script>window.location.href = 'https://secured-login.net/pages/10ab5b62ac22/XTlU1aGJteE9NRk5DU0ZCUVNucGlTRkJCZDJGTVZXTlRjR29yZUdrMFZrdGpURFI2ZURJMUwzbzVWV3hyY21sT1pHNXdRVVYwTkhkWmFVOVBUalpaTDBwUVZESk1abTkyZFRscE0za3lSRWt3ZEUxU1ZHWnJURzVXZFhONksySkJRVmxKVFVWVWRtMVJaekZCY2xWWVJWRTNWbE14WmpoV2QxZGxRa280VlZaUldrUjNZbWR6T1dod1dUQndSRkpJT1ZocFZ6VnJLekIwVGtKU1luZzVWMWxYY21wQ1luVjJRa28wUFMwdFZ5ODJka0pTTVdkcFFURk5hSEExVWtaTmRIWnFkejA5LS1mNTY3M2RlODQzYTFhY2IwZTFjOTZiNGQ1YjI3MTU0NDk0YTgzNDVl';</script>. </head>. <body>. </body>.</html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\Microsoft-Logo-PNG[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1870 x 690, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	11903
Entropy (8bit):	7.570735023271992

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\Microsoft-Logo-PNG[1].png	
Encrypted:	false
SSDEEP:	192:SU1111111f1111ba8SwLOMuhKM+2K5en7OhLFuZYdWR9jPws0IUyuFm9Q2v1111J:SH8SnYZ2K5en7OJFsiu9jb0IFOm9Q2h
MD5:	9A33A3A3F48640338BEBF18657DEAA2D
SHA1:	3E66B927D14625DA739CA160FE32B30E603D786B
SHA-256:	B89BE8A1426FB07A01CC6F865B33F447BA12BB09A02EE1535AB9FFFDB3DADC66
SHA-512:	998FCA3F2FDF8ACF802CCA64369938F40EE41D3BE0E29D0C523A42F3C5B265C8AF2378DCDF968084D43DF0F50EDFB3F6554BEC479E0F8227E9C2F811A9F115E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ctsciencecenter.org/wp-content/uploads/2017/08/Microsoft-Logo-PNG.png
Preview:	.PNG.....IHDR...N.....e.....ZPLTE.....ppppppuuutttsssrrrttttttt...sss....P"...sssrrr...ttt....P#...sssssssss...sss....P".....K.....tRNS... 0@P`p.....WBX...-.IDATx...Q..... Q..1!.^v.&N...f.{..v.T.BH .s.....c>$.>.7.`..M..r..r..r...)..)..). .. ..r..r..r..r...)..)..). .. ..r..r..r..r...)..)..). .. ..r..r..r..r...)..)..). .. ..r..r..r..r...)..)..). .. ..r..r..r..r...)..)..). .. ..r..r..r..r...)..)..). .. ..r..r..r..r...)..)..). .. ..r..r..r..r...)..)..). .. ..r..r..r..r...)..)..). .. ..r..r..r..r...)..)..). .. ..r..r..r.....{..q...s..n...S9.S..TN..S9.@N.TN..TN...9 .S..TN..S9.S.9.S9.@N...9.S..TN..@N.TN..S9.@N...9.S9..S9.S..TN..S9.@N.TN..TN...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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\WJ8I2OL4\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\Temp\~DF46A2DCC3BAE2745C.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13077
Entropy (8bit):	0.5117719476712306

C:\Users\user\AppData\Local\Temp\~DF46A2DCC3BAE2745C.TMP	
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loCF9lo+9lWfuOmyugLB:kBqoIJffNmyugLB
MD5:	DC6B2C492092375D9AB1C9877B2DE650
SHA1:	01023BC04D6E4BB4CE613A89B2E34E315A4D0DFE
SHA-256:	A0A7CCAC646EC7513CB01FBEDFE302E171311FEC03A31816B74B7BBC1EA4DD5A
SHA-512:	B88A3B0C612140A610221CB26CD6F19A46EE8FE46F463251CFFA0E50A55D43AD12DFD5B7C52A7F0BDE4D8F0563EF12DFD9CD90B13A21A3C02F2B87B80360CF C0
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFA1630E5320976778.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.8214419358848888
Encrypted:	false
SSDEEP:	48:kBqoxxJhHWSVSEab2W966ZLchcYwQ3YH3eaAT/cYwQ3YH3aPa7/ck:kBqoxDhHWSVSE+1Gh5tgK/5tgaw/P
MD5:	637F8165FFF71A41EB0D8526482BD81E
SHA1:	AA2DB01EBCB22C27970770F30EE808A5AF604AC0
SHA-256:	413526EF7900B553342426386B11200F471EC584FDFAA1939C6C14DAA9C1762A
SHA-512:	43C1AB0CF432EE8A41EEB82E42156A21D6F0279F6824490F06B6B1889D3D2174EF98ABBBD23E0875AEE305D168D6DEFC7D4B38EAA6F4992A6D42658427524AF 7
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFABA5B5234A7FE127.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	48188
Entropy (8bit):	1.6606221597570698
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+357yZJ2bg7abgi/EbgZbgI8bgxbgvbgKbgpbgrbgsbg:kBqoxKAuqR+357yZJ2KaLEo/8c6vke5
MD5:	E9B37BDF34BBDC70BC009281C961C9B8
SHA1:	5033074313789C4DB078485760304A6E3EB199D9
SHA-256:	B7E46DA54E6E28A51586EF260BFA668D8DC7C1AA951D49EBBB4C87D6B02D8A64
SHA-512:	388826824C2E3BBA54B4E97900A2C9E2C8BFFB7ECFA7B798C8C78BF92C22A85F2A5E13B990967221A17A8486D33266CD09E1CB2852C85EB7024C59475880D056
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

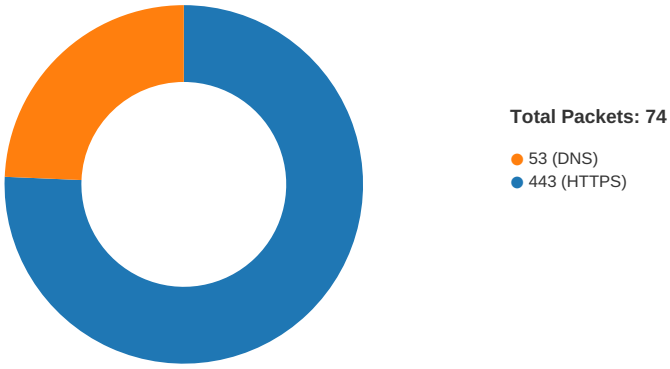
Static File Info

No static file info

Network Behavior

Network Port Distribution

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 06:39:07.323807001 CEST	49711	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.324609041 CEST	49712	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.451096058 CEST	443	49711	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:07.451245070 CEST	49711	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.452281952 CEST	443	49712	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:07.452425003 CEST	49712	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.456522942 CEST	49711	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.457740068 CEST	49712	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.586416006 CEST	443	49711	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:07.587306023 CEST	443	49711	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:07.587336063 CEST	443	49711	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:07.587359905 CEST	443	49711	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:07.587385893 CEST	443	49711	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:07.587389946 CEST	49711	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.587404966 CEST	443	49711	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:07.587414980 CEST	49711	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.587420940 CEST	49711	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.587445021 CEST	49711	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.587472916 CEST	49711	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.587968111 CEST	443	49712	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:07.588891029 CEST	443	49712	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:07.588927984 CEST	443	49712	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:07.588958025 CEST	443	49712	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:07.588985920 CEST	443	49712	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:07.589004040 CEST	443	49712	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:07.589085102 CEST	49712	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.589126110 CEST	49712	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.589133024 CEST	49712	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.589137077 CEST	49712	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.618062019 CEST	49711	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.618217945 CEST	49712	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.624375105 CEST	49711	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.624655962 CEST	49711	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.624695063 CEST	49712	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.745379925 CEST	443	49711	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:07.745455980 CEST	443	49711	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:07.745492935 CEST	49711	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.745569944 CEST	49711	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.745960951 CEST	443	49712	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:07.745992899 CEST	443	49712	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:07.746083975 CEST	49712	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.746144056 CEST	49712	443	192.168.2.3	54.175.141.245

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 06:39:07.746943951 CEST	49712	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.747157097 CEST	49711	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.751274109 CEST	443	49711	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:07.751449108 CEST	49711	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.752005100 CEST	443	49712	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:07.752161980 CEST	49712	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.792959929 CEST	443	49711	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:07.835413933 CEST	443	49711	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:07.835442066 CEST	443	49711	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:07.835602999 CEST	49711	443	192.168.2.3	54.175.141.245
Apr 12, 2021 06:39:07.874079943 CEST	443	49711	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:07.918175936 CEST	443	49712	54.175.141.245	192.168.2.3
Apr 12, 2021 06:39:08.068048954 CEST	49715	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.068048954 CEST	49714	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.195337057 CEST	443	49715	52.22.122.101	192.168.2.3
Apr 12, 2021 06:39:08.195511103 CEST	49715	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.196176052 CEST	49715	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.196253061 CEST	443	49714	52.22.122.101	192.168.2.3
Apr 12, 2021 06:39:08.196355104 CEST	49714	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.197128057 CEST	49714	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.325287104 CEST	443	49715	52.22.122.101	192.168.2.3
Apr 12, 2021 06:39:08.326076984 CEST	443	49715	52.22.122.101	192.168.2.3
Apr 12, 2021 06:39:08.326117992 CEST	443	49715	52.22.122.101	192.168.2.3
Apr 12, 2021 06:39:08.326157093 CEST	443	49715	52.22.122.101	192.168.2.3
Apr 12, 2021 06:39:08.326195002 CEST	443	49715	52.22.122.101	192.168.2.3
Apr 12, 2021 06:39:08.326195955 CEST	49715	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.326224089 CEST	443	49715	52.22.122.101	192.168.2.3
Apr 12, 2021 06:39:08.326256037 CEST	49715	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.326261997 CEST	49715	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.326293945 CEST	49715	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.326297998 CEST	49715	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.326308012 CEST	443	49714	52.22.122.101	192.168.2.3
Apr 12, 2021 06:39:08.327338934 CEST	443	49714	52.22.122.101	192.168.2.3
Apr 12, 2021 06:39:08.327382088 CEST	443	49714	52.22.122.101	192.168.2.3
Apr 12, 2021 06:39:08.327419996 CEST	443	49714	52.22.122.101	192.168.2.3
Apr 12, 2021 06:39:08.327429056 CEST	49714	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.327457905 CEST	443	49714	52.22.122.101	192.168.2.3
Apr 12, 2021 06:39:08.327461958 CEST	49714	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.327475071 CEST	49714	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.327486992 CEST	443	49714	52.22.122.101	192.168.2.3
Apr 12, 2021 06:39:08.327527046 CEST	49714	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.327549934 CEST	49714	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.352266073 CEST	49715	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.352683067 CEST	49715	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.352883101 CEST	49715	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.355171919 CEST	49714	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.355607986 CEST	49714	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.481504917 CEST	443	49715	52.22.122.101	192.168.2.3
Apr 12, 2021 06:39:08.481553078 CEST	443	49715	52.22.122.101	192.168.2.3
Apr 12, 2021 06:39:08.481621027 CEST	49715	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.481662035 CEST	49715	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.481662989 CEST	443	49715	52.22.122.101	192.168.2.3
Apr 12, 2021 06:39:08.481739044 CEST	49715	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.482883930 CEST	49715	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.484683037 CEST	443	49714	52.22.122.101	192.168.2.3
Apr 12, 2021 06:39:08.484714031 CEST	443	49714	52.22.122.101	192.168.2.3
Apr 12, 2021 06:39:08.484837055 CEST	49714	443	192.168.2.3	52.22.122.101
Apr 12, 2021 06:39:08.484882116 CEST	49714	443	192.168.2.3	52.22.122.101

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 06:38:59.589272976 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 12, 2021 06:38:59.638350964 CEST	53	60152	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 06:39:00.290273905 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 12, 2021 06:39:00.356091022 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 12, 2021 06:39:00.481626034 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 12, 2021 06:39:00.530488968 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 12, 2021 06:39:03.454173088 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 12, 2021 06:39:03.514287949 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 12, 2021 06:39:04.850531101 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 12, 2021 06:39:04.907778978 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 12, 2021 06:39:06.221604109 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 12, 2021 06:39:06.281521082 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 12, 2021 06:39:06.446650028 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 12, 2021 06:39:06.495563030 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 12, 2021 06:39:07.226530075 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 12, 2021 06:39:07.305871964 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 12, 2021 06:39:07.596357107 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 12, 2021 06:39:07.649008989 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 12, 2021 06:39:08.008636951 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 12, 2021 06:39:08.066035032 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 12, 2021 06:39:08.703433037 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 12, 2021 06:39:08.796890974 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 12, 2021 06:39:08.811830997 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 12, 2021 06:39:08.860543966 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 12, 2021 06:39:11.389027119 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 12, 2021 06:39:11.468978882 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 12, 2021 06:39:12.757299900 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 12, 2021 06:39:12.810218096 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 12, 2021 06:39:22.722981930 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 12, 2021 06:39:22.780509949 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 12, 2021 06:39:23.455302954 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 12, 2021 06:39:23.514905930 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 12, 2021 06:39:23.923723936 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 12, 2021 06:39:23.973083019 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 12, 2021 06:39:32.871584892 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 12, 2021 06:39:33.120466948 CEST	53	57568	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 06:39:07.226530075 CEST	192.168.2.3	8.8.8.8	0x2320	Standard query (0)	welsfargo.com-onlinebanking.com	A (IP address)	IN (0x0001)
Apr 12, 2021 06:39:08.008636951 CEST	192.168.2.3	8.8.8.8	0x486d	Standard query (0)	secured-login.net	A (IP address)	IN (0x0001)
Apr 12, 2021 06:39:08.703433037 CEST	192.168.2.3	8.8.8.8	0x2e7f	Standard query (0)	ctsciencecenter.org	A (IP address)	IN (0x0001)
Apr 12, 2021 06:39:11.389027119 CEST	192.168.2.3	8.8.8.8	0xa4b6	Standard query (0)	logincdn.msauth.net	A (IP address)	IN (0x0001)
Apr 12, 2021 06:39:23.455302954 CEST	192.168.2.3	8.8.8.8	0xe981	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
Apr 12, 2021 06:39:07.305871964 CEST	8.8.8.8	192.168.2.3	0x2320	No error (0)	welsfargo.com-online banking.com	landing.training.knowbe4.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 06:39:07.305871964 CEST	8.8.8.8	192.168.2.3	0x2320	No error (0)	landing.training.knowbe4.com		54.175.141.245	A (IP address)	IN (0x0001)
Apr 12, 2021 06:39:07.305871964 CEST	8.8.8.8	192.168.2.3	0x2320	No error (0)	landing.training.knowbe4.com		54.174.93.80	A (IP address)	IN (0x0001)
Apr 12, 2021 06:39:07.305871964 CEST	8.8.8.8	192.168.2.3	0x2320	No error (0)	landing.training.knowbe4.com		3.229.61.65	A (IP address)	IN (0x0001)
Apr 12, 2021 06:39:07.305871964 CEST	8.8.8.8	192.168.2.3	0x2320	No error (0)	landing.training.knowbe4.com		54.166.42.17	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 06:39:07.305871964 CEST	8.8.8.8	192.168.2.3	0x2320	No error (0)	landing.trainingknowbe4.com		52.44.64.207	A (IP address)	IN (0x0001)
Apr 12, 2021 06:39:07.305871964 CEST	8.8.8.8	192.168.2.3	0x2320	No error (0)	landing.trainingknowbe4.com		52.22.122.101	A (IP address)	IN (0x0001)
Apr 12, 2021 06:39:08.066035032 CEST	8.8.8.8	192.168.2.3	0x486d	No error (0)	secured-login.net		52.22.122.101	A (IP address)	IN (0x0001)
Apr 12, 2021 06:39:08.066035032 CEST	8.8.8.8	192.168.2.3	0x486d	No error (0)	secured-login.net		3.229.61.65	A (IP address)	IN (0x0001)
Apr 12, 2021 06:39:08.066035032 CEST	8.8.8.8	192.168.2.3	0x486d	No error (0)	secured-login.net		54.175.141.245	A (IP address)	IN (0x0001)
Apr 12, 2021 06:39:08.066035032 CEST	8.8.8.8	192.168.2.3	0x486d	No error (0)	secured-login.net		52.44.64.207	A (IP address)	IN (0x0001)
Apr 12, 2021 06:39:08.066035032 CEST	8.8.8.8	192.168.2.3	0x486d	No error (0)	secured-login.net		54.166.42.17	A (IP address)	IN (0x0001)
Apr 12, 2021 06:39:08.066035032 CEST	8.8.8.8	192.168.2.3	0x486d	No error (0)	secured-login.net		54.174.93.80	A (IP address)	IN (0x0001)
Apr 12, 2021 06:39:08.796890974 CEST	8.8.8.8	192.168.2.3	0x2e7f	No error (0)	ctsciencecenter.org		104.131.254.50	A (IP address)	IN (0x0001)
Apr 12, 2021 06:39:11.468978882 CEST	8.8.8.8	192.168.2.3	0xa4b6	No error (0)	logincdn.msauth.net	lgincdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 06:39:11.468978882 CEST	8.8.8.8	192.168.2.3	0xa4b6	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)
Apr 12, 2021 06:39:23.514905930 CEST	8.8.8.8	192.168.2.3	0xe981	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
Apr 12, 2021 06:39:07.587385893 CEST	54.175.141.245	443	192.168.2.3	49711	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
Apr 12, 2021 06:39:07.588985920 CEST	54.175.141.245	443	192.168.2.3	49712	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		
Apr 12, 2021 06:39:08.326195002 CEST	52.22.122.101	443	192.168.2.3	49715	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
Apr 12, 2021 06:39:08.327457905 CEST	52.22.122.101	443	192.168.2.3	49714	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		
Apr 12, 2021 06:39:09.056608915 CEST	104.131.254.50	443	192.168.2.3	49716	CN=ctsciencecenter.org CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Mar 22 16:55:48 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Sun Jun 20 17:55:48 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Apr 12, 2021 06:39:09.057625055 CEST	104.131.254.50	443	192.168.2.3	49717	CN=ctsciencecenter.org CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Mar 22 16:55:48 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Sun Jun 20 17:55:48 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Apr 12, 2021 06:39:11.560009956 CEST	192.229.221.185	443	192.168.2.3	49719	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, 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	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 CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jul 20 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Tue Jul 20 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=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		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Apr 12, 2021 06:39:11.560265064 CEST	192.229.221.185	443	192.168.2.3	49720	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, 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	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 CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jul 20 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Tue Jul 20 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	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		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5780 Parent PID: 792

General

Start time:	06:39:05
Start date:	12/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff76f7a0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 5248 Parent PID: 5780

General

Start time:	06:39:06
Start date:	12/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5780 CREDAT:17410 /prefetch:2
Imagebase:	0x210000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly