ID: 348682
Cookbook: browseurl.jbs
Time: 14:32:48
Date: 04/02/2021
Version: 31.0.0 Emerald

Table of Contents

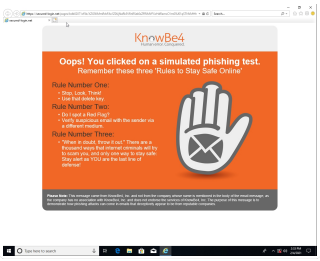
Analysis Report https://covid19.protected-forms.com/XZ…

Overview

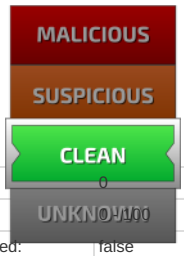
General Information

Sample URL:	https://covid19.protected-forms.com/XZG5KMmRrbFJla1Z0UjNaRk5VRnRSek0zZFRJMV...jQyWmxBd1MwZHVkejA5LS00NjA2MjUyNDMxYTNlYmY0ZmIyOTgxY2NjZGM0MjQzMjk2MzUwNDdm
Analysis ID:	348682

Most interesting Screenshot:



Detection

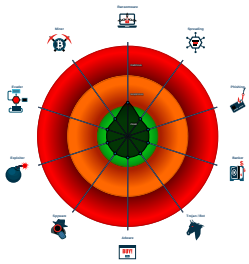


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 7040 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 7088 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7040 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

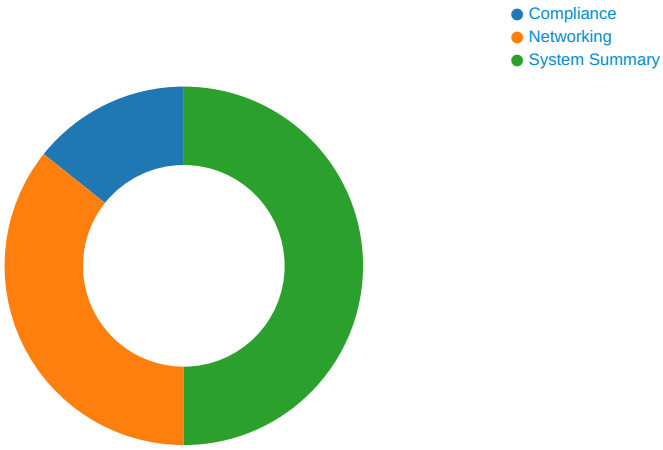
Yara Overview

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.

Compliance:

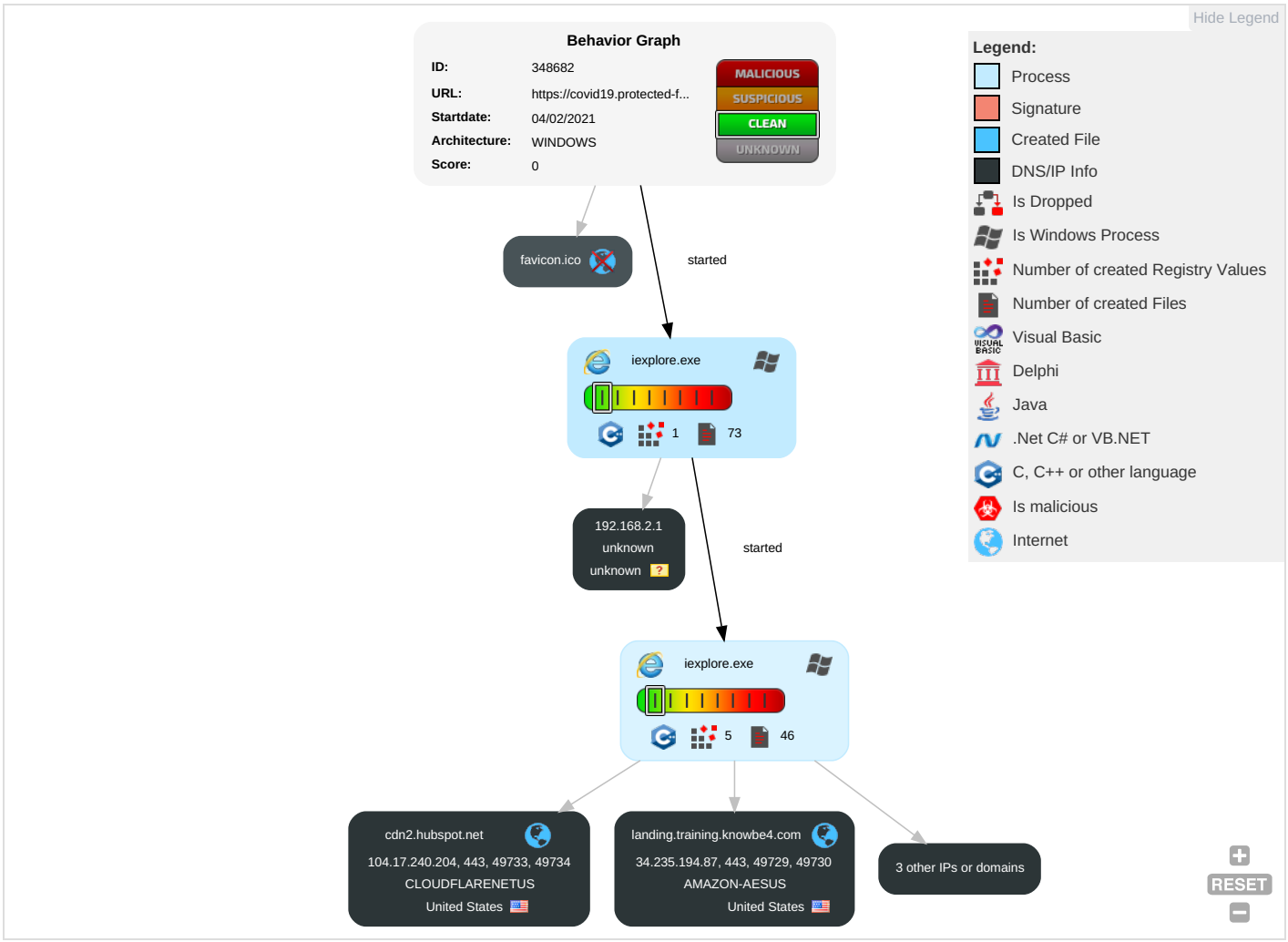
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

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

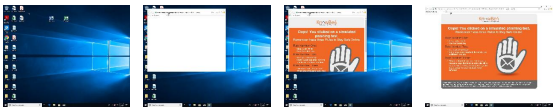
Behavior Graph

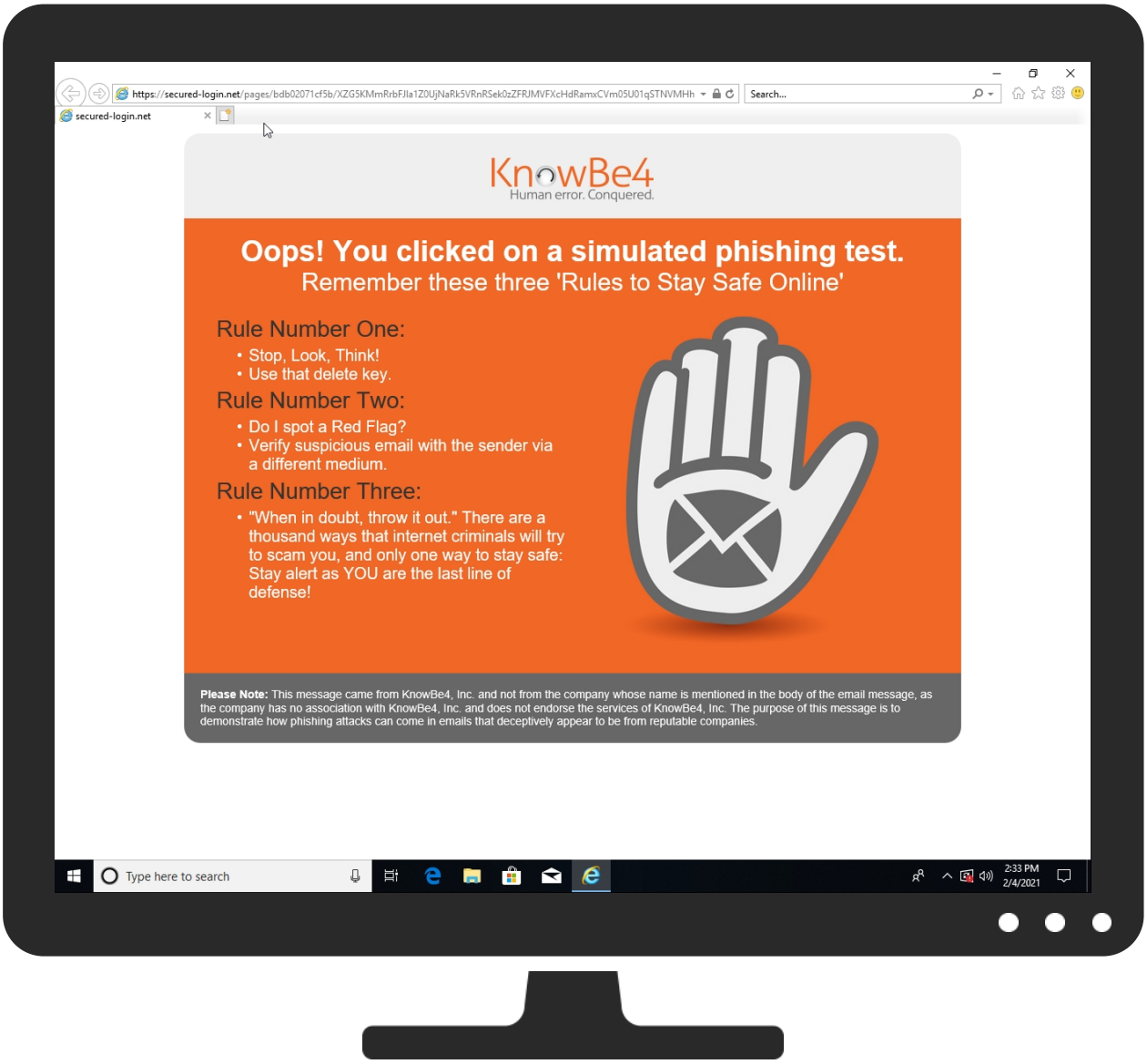


Screenshots

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/XZG5KMmRrbFJla1Z0UjNaRk5VRnRSek0zZFRJMVFXcHdRamxCVm05U01qSTNVMHhvS3pCd2VXYzJiMjlKU0RKV2VUSnpaSGhZUWl0SWFGaE5TRTlyT0dGeGJGVXpOME5HVEcxMk9DOXZNVFk1SzJnMFEwaHBhRUlyUWs5UFVuUlpRMVJhTjBsVFRFczJlVTVwYm1WRWRrWlJZVlJ0VDBZM1dXZ3dXVmd5Y0hBM1pTOVJPVkF4VVc0eWJtTnZibk50WkdSTmRESllPRFV2TlZadlJDOHJaRXcyYUhVNVdrTXhXRlJCUFMwdE5HUmpkMUpVVGs1WE9WUXdZMjQyWmxBd1MwZHVkejA5LS00NjA2MjUyNDMxYTNlYmY0ZmIyOTgxY2NjZGM0MjQzMjk2MzUwNDdm	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://secured-login.ted-forms.com/XZG5KMmRrbFJla1Z0UjNaRk5VRnRSek0zZFRJMVFXcHdRamxCVm05U01qSTNVMHh	0%	Avira URL Cloud	safe	
http://https://w3c.github.io/IntersectionObserver/#intersection-observer-interface	0%	Avira URL Cloud	safe	
http://docs.closure-library.googlecode.com/git/closure_goog_date_date.js.source.html	0%	Avira URL Cloud	safe	
http://https://www.nathanaeluser.com/blog/2013/reading-max-width-cross-browser	0%	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%	Avira URL Cloud	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
cdn2.hubspot.net	104.17.240.204	true	false		high
s3.amazonaws.com	52.216.170.5	true	false		high
secured-login.net	52.203.61.30	true	false		unknown
landing.training.knowbe4.com	34.235.194.87	true	false		high
covid19.protected-forms.com	unknown	unknown	false		unknown
favicon.ico	unknown	unknown	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://api.jqueryui.com/slide-effect/	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/moment/moment/issues/1423	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/chartjs/Chart.js/pull/4507	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://stackoverflow.com/a/32954565/96342	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/madrobby/zepto/blob/master/src/zepto.js	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://https://stackoverflow.com/questions/30464750/chartjs-line-chart-set-background-color	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/chartjs/Chart.js/issues/5597	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://stackoverflow.com/a/26707753	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/jquery/jquery-color	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/select2/select2/blob/master/LICENSE.md	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://api.jqueryui.com/jQuery.widget/	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://blog.jquery.com/2012/08/09/jquery-1-8-released/	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://codereview.stackexchange.com/q/13338	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high

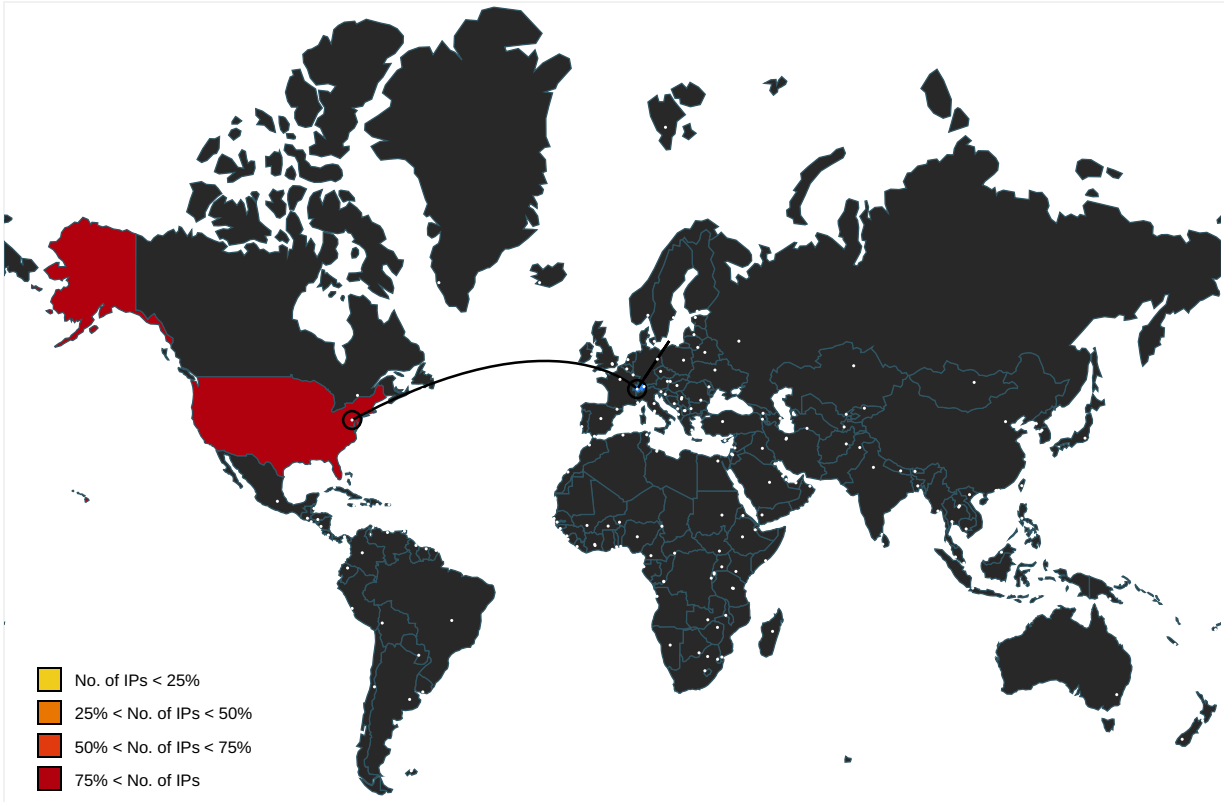
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn2.hubspot.net/hubfs/241394/html_file/files/img/KB4-logo.png	PGA2OXVV.htm.2.dr	false		high
http://https://secured-login.ted-forms.com/XZG5KMmRrbFJla1Z0UjNaRk5VRnRSek0zZFRJMVFXcHdRamxCVm05U01qSTNVMHh	{96F6E6C4-66ED-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://bugzilla.mozilla.org/show_bug.cgi?id=561664	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://dev.w3.org/csswg/cssom/#resolved-values	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://https://caniuse.com/download	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/chartjs/Chart.js/issues/2538	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://dev.w3.org/csswg/css-color/#hwb-to-rgb	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/jrburke/requirejs/wiki/Updating-existing-libraries#wiki-anon	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://www.apache.org/licenses/LICENSE-2.0)	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/kriskowal/es5-shim/blob/master/es5-shim.js	modernizr-79e0181ec91aff04bb01d87cba546535ede843f75d19f5c60f66b8dd6546971f[1].js.2.dr	false		high
http://api.jqueryui.com/button/	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://https://bugzilla.mozilla.org/show_bug.cgi?id=687787	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://https://blog.alexmaccaw.com/css-transitions	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/bassjobsen/Bootstrap-3-Typeahead	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://https://getbootstrap.com/docs/3.4/javascript/#transitions	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/chartjs/Chart.js/issues/4152	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://bugs.jquery.com/ticket/9917	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://api.jqueryui.com/size-effect/	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/Do/iso8601.js	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://https://developer.mozilla.org/en-US/docs/Web/API/EventTarget/addEventListener#Safely_detecting_optio	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://momentjs.com/guides/#/warnings/zone/	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://bugs.jquery.com/ticket/12359	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://https://developer.mozilla.org/en-US/docs/Web/API/EventTarget/removeEventListener	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://https://w3c.github.io/IntersectionObserver/#intersection-observer-interface	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://creativecommons.org/licenses/by/3.0/)	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false		high
http://docs.closure-library.googlecode.com/git/closure_goog_date_date.js.source.html	application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[1].js.2.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.nathanaeluser.com/blog/2013/reading-max-width-cross-browser	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/truckingsim/Ajax-Bootstrap-Select	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://bugzilla.mozilla.org/show_bug.cgi?id=649285	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://getbootstrap.com/docs/3.4/javascript/#tooltip	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/chartjs/Chart.js/issues/6104	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://jsperf.com/diacritics/18	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://api.jqueryui.com/category/ui-core/	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/twbs/bootstrap/issues/20280	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/chartjs/Chart.js/issues/4287	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://getbootstrap.com/docs/3.4/javascript/#modals	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http:// https://github.com/chartjs/Chart.js/issues/2435#issuecomment-216718158	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://jsperf.com/object-keys-vs-for-in-with-closure/3	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://stackoverflow.com/q/181348	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://getbootstrap.com/docs/3.4/javascript/#collapse	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://www.anujgakhar.com/2014/03/01/binary-search-in-javascript/	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/chartjs/Chart.js/issues/4737	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/kkapsner/CanvasBlocker	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://www.robertpenner.com/easing/	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://w3c.github.io/IntersectionObserver/#calculate-intersection-rect-algo	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/chartjs/Chart.js/issues/3887	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://getbootstrap.com/docs/3.4/javascript/#scrollspy	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/w3c/IntersectionObserver/issues/211	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://flightschool.acylt.com/devnotes/caret-position-woes/	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://api.jqueryui.com/transfer-effect/	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/rails/jquery-ujs	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://stackoverflow.com/questions/8506881/nice-label-algorithm-for-charts-with-minimum-ticks	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://bugzilla.mozilla.org/show_bug.cgi?id=491668	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/marcj/css-element-queries	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://www.robertpenner.com/easing)	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://momentjs.com/guides/#/warnings/min-max/	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/truckingsim/Ajax-Bootstrap-Select/issues/155	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/truckingsim/Ajax-Bootstrap-Select/issues/156	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/truckingsim	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http:// https://s3.amazonaws.com/helpimg/landing_pages/images/stoplookthink.jpg	PGA2OXVV.htm.2.dr	false		high
http://https://github.com/chartjs/Chart.js/issues/4102	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://stackoverflow.com/q/3922139	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://api.jqueryui.com/drop-effect/	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://www.amazon.com/	msapplication.xml.1.dr	false		high
http://stackoverflow.com/questions/846221/logarithmic-slider	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://www.twitter.com/	msapplication.xml5.1.dr	false		high
http://jsperf.com/getall-vs-sizzle/2	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://getbootstrap.com/docs/3.4/javascript/#buttons	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/jquery/jquery/pull/557)	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://www.html5canvastutorials.com/advanced/html5-canvas-mouse-coordinates/	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://api.jqueryui.com/menu/	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://getbootstrap.com/docs/3.4/javascript/#alerts	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/chartjs/Chart.js/issues/5208	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://api.jqueryui.com/category/effects-core/	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://bugs.jquery.com/ticket/8235	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http:// https://chartjs.gitbooks.io/proposals/content/Platform.html	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://api.jqueryui.com/dialog/	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://w3c.github.io/IntersectionObserver/#intersection-observer-entry	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://api.jqueryui.com/shake-effect/	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://https://github.com/Microsoft/tslib/blob/v1.6.0/tslib.js	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://stackoverflow.com/questions/10149963/adding-event-listener-cross-browser	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/markcarver	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://https://github.com/imulus/retinajs/issues/8	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high
http://jsperf.com/1-vs-infinity	application-ae943aec8610a8eb1c b217c05ea40d5860932dc46d4205e7 0b987b3f81ea9e34[1].js.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.235.194.87	unknown	United States		14618	AMAZON-AESUS	false
52.203.61.30	unknown	United States		14618	AMAZON-AESUS	false
52.216.170.5	unknown	United States		16509	AMAZON-02US	false
104.17.240.204	unknown	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	348682
Start date:	04.02.2021
Start time:	14:32:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://covid19.protected-forms.com/XZG5KMmRrbFJla1Z0UjNaRk5VRnRSek0zZFRJMVFXcHdRamxCVm05U01qSTNVMHhvS3pCd2VXYzJiMjlKU0RKV2VUSnpaSGhZUWl0SWFGaE5TRTlyT0dGeGJGVXpOME5HVEcxMk9DOXZNVFk1SzJnMFEwaHBhRUlyUWs5UFVuUlpRMVJhTjBsVFRFczJlVTVwYm1WRWRrWlJZVlJ0VDBZM1dXZ3dXVmd5Y0hBM1pTOVJPVkF4VVc0eWJtTnZibk50WkdSTmRESllPRFV2TlZadlJDOHJaRXcyYUhVNVdrTXhXRlJCUFMwdE5HUmpkMUpVVGs1WE9WUXdZMjQyWmxBd1MwZHVkejA5LS00NjA2MjUyNDMxYTNlYmY0ZmIyOTgxY2NjZGM0MjQzMjk2MzUwNDdm
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@3/24@5/5
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 88.221.62.148, 13.64.90.137, 104.43.193.48, 40.88.32.150, 51.11.168.160, 168.61.161.212, 92.122.213.247, 92.122.213.194, 152.199.19.161, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, ie9comview.vo.msecnd.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, go.microsoft.com.edgekey.net, blobcollector.events.data.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, cs9.wpc.v0cdn.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\E5F0NRSV\secured-login[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	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.{96F6E6C2-66ED-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8548251725922054
Encrypted:	false
SSDEEP:	192:r2XZBZi2a9W5Zt5V2if5mZnzMhufBdRlDdGsfdiZGjX:r2JHBaU5bHp4RjV
MD5:	7329C430E77C8AA767DBB6B1BCFA8F71
SHA1:	6A60216579F89013607FF6C954709EF3CFAB0D76
SHA-256:	20E7000EEB3B8A288C6A49E28D6F0D120CE1EAEB171406529AB2A8619E5D698A
SHA-512:	D3A752B67805BC6C78F30613ABA9400A38B983D7840F6B876F3EB778EDD5E92C0841197068FBC6A19E93B8A5B50EB7BC78F9620E11CA8877BA900C95BE5F491
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\{96F6E6C4-66ED-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	36514
Entropy (8bit):	2.5379834203101366
Encrypted:	false
SSDEEP:	192:rwXZBQ9z6DkIFj9T2OkWtMEYAhRSu/IRSFRARS6RSOiRSWRSQRSwRSzRSmkg:rwJW9WIIhEq+EphfIealniZnXcBv
MD5:	E2D335E1EF95C20E5B88DDEF94BAB1A1
SHA1:	0AB9752DA7EE41DEEF06169F0BB1E8BAA82C34C1
SHA-256:	B0B6D945BEF2EB9C3DDDD5969A83557AE791F163C853498AFB2C971CF25473FC
SHA-512:	A353E1744EF00442A0FCE2A0FCF7D646F6697FFA561B916979ECD0DE3B573A579D2CD8EB93D38FABC4ED92F6E17DE050FE72962BC6FE47F078717155B8A081E E
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\{9D855CE8-66ED-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.566287262826108
Encrypted:	false
SSDEEP:	48:IwKGcprDGwpaPG4pQfGrapbSHErGQpKDG7HpRjsTGIpG:ruZdQB6jBSHEFASTj4A
MD5:	6B3EBB107D1977FC63201ACA106A9EB4
SHA1:	F4C41D165E4C2430C6B597B3FE7EE3A20910FB95
SHA-256:	3486DD29C444EF696F73381A5FB09D68EB8AC8271DCA5A3E453749285E4A76E7
SHA-512:	44E05E943A4BABF9044466DC365B5B3D4B1F0FBF9524F9FD0BF7B639352D89D272C6428BCA94BD71988AE796E74CFFE322901FB36656758C32C0BB46F6CE63C
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):	5.044657917658642
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEiRxRqnWimI002EtM3MHdNMNxOEiRxRqnWimI00OYGVbkEtMb:2d6NxOdbQSZHKd6NxOdbQSZ7YLb
MD5:	2452E44BDDD159C56A59B25DB5851239
SHA1:	A69D1980F7E11BFAAD7B3EFD710712038DF08200
SHA-256:	8B86346CD0559B0BA9C77A7456DEC36BB76BB93D282A8FD151329DE2BF2C3DE2
SHA-512:	DBDBF4CA1EE99632E1C99F47A88C9B84D43C30E17A2AFE1C479C5FE647D2F689A3D97CE3B50DE049A0483CD3D1B54BAE6DCA9FEB2EE825B8A2A2065F62131 13B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x6e70d2e6,0x01d6fafa</date><accdate>0x6e70d2e6,0x01d6fafa</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>0x6e70d2e6,0x01d6fafa</date><accdate>0x6e70d2e6,0x01d6fafa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.058197115918378
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
SSDEEP:	12:TMHdNMNxe2kD1lf1lPnWimI002EtM3MHdNMNxe2kD1lf1lPnWimI00OYGkak6Ety:2d6Nxr6lNlPSZHKd6Nxr6lNlPSZ7Yzan
MD5:	7B64DA8270EBAA6B31A2356A386CF319
SHA1:	F9DA76043B5C2634EA891F21EAB03E5293C2093F
SHA-256:	99E8D991D96EBAB8AA259A522E48197B57EFE4A29D8986667A836DC27687D4AB
SHA-512:	C62AD8C1C3388F7ACC95FA8E1C7930E6DBD1D9CFFC7C30CAE15C60EB4411F1E27B853881137B480597CA5EE17061FEF76CB01E9085AF5278C415F3CC0F8CAE EC
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x6e6c0e75,0x01d6fafa</date><a ccdate>0x6e6c0e75,0x01d6fafa</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>0x6e6c0e75,0x01d6fafa</date><a ccdate>0x6e6c0e75,0x01d6fafa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Am azon.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):	5.092483126987695
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL5+S+qnWimI002EtM3MHdNMNxvL5+S+qnWimI00OYGmZEtMb:2d6Nxv3SZHKd6Nxv3SZ7Yjb
MD5:	3A07E03EB87EB9F44F668028FA0F0543
SHA1:	C547EDCBD32FD26C517A9B36A710883BF2EC9ACE
SHA-256:	2EF291B539907ABF796EF4323CB476E263F0DA0BBC415AA7FD56035C155CE051
SHA-512:	4F550295E370EB745029AC7995C8AC862FEAFCF0B56633571CF1D7A3FAD5DDB5AB915B895D5E30CF03782387D97CAD8C917A326A903DF987E41DF265FF33D24
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x6e73354f,0x01d6fafa</date> <accdate>0x6e73354f,0x01d6fafa</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>0x6e73354f,0x01d6fafa</date><accda te>0x6e73354f,0x01d6fafa</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):	5.040873586738572
Encrypted:	false
SSDEEP:	12:TMHdNMNxiA8vnWimI002EtM3MHdNMNxiA8vnWimI00OYGd5EtMb:2d6Nxz8vSZHKd6Nxz8vSZ7YEjb
MD5:	B41C99BAF1C6067C50AB0BA2077736DE
SHA1:	E6BD03CAE5E8680A3EE7ECA1725016292E195935
SHA-256:	F11D074499312B9205C5F91745E9B0576F51CFC34450834D451F00E0130DFE3A
SHA-512:	C8E3C93EB0C20F155F1CFA5496ADE6E9E32E24BE9E27560106307EAE367B48078B86626147F0AD151429C93EE7E5AEDED41EC84D2B021B5763FA1FB5DD881BC C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x6e6e70ab,0x01d6fafa</date><acc date>0x6e6e70ab,0x01d6fafa</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>0x6e6e70ab,0x01d6fafa</date><accdate>0x6e6e7 0ab,0x01d6fafa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msappl ication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.107949956001045
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw5+S+qnWimI002EtM3MHdNMNxhGw5+S+qnWimI00OYG8K075EtMb:2d6NxQWSZHKd6NxQWSZ7YrKajb
MD5:	D942A3C919EA5B5D0D18E4EAFEEA66B2
SHA1:	EB05AB877A4B9065440766A3179DFCE9EBCC2835
SHA-256:	B005843284163CEA5AE5DCEDDE2465CC7577C9115B9406D65AA5E0EF2DFC19EC

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
SHA-512:	A2996095BA79ED4835FD4F0DBBE91CF5D9E658A40ADC46EACCE77E018D48BF060B7A2C7282B93FE8C66F658382898C0C6282A5F7BC4A13051210967B959EA8E7
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x6e73354f,0x01d6fafa</date><accdate>0x6e73354f,0x01d6fafa</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>0x6e73354f,0x01d6fafa</date><accdate>0x6e73354f,0x01d6fafa</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):	5.045643438633671
Encrypted:	false
SSDEEP:	12:TMHdNMNx0niRxRqnWimI002EtM3MHdNMNx0niRxRqnWimI00OYGxEtMb:2d6Nx0ibQSZHKd6Nx0ibQSZ7Ygb
MD5:	28C0C4850B3B744A68A3D6A2973E941C
SHA1:	CFB269BD99CF4AE594B6BC56AB6A6687AB29298F
SHA-256:	F8846C9A3013A9E669472FAA010093848FE922C34977BEC6202E6EBBA6BCDB8D
SHA-512:	C222942E32931ED400F5A883A659B188EB1EE72FE2CA3BDBED3DCC19A9284408A996079FC4718BF406830593293CB425214B5432425550AAB387F3DA0DFA5CB2
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x6e70d2e6,0x01d6fafa</date><accdate>0x6e70d2e6,0x01d6fafa</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>0x6e70d2e6,0x01d6fafa</date><accdate>0x6e70d2e6,0x01d6fafa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.084293196986436
Encrypted:	false
SSDEEP:	12:TMHdNMNxxiRxRqnWimI002EtM3MHdNMNxxiRxRqnWimI00OYG6Kq5EtMb:2d6NxYbQSZHKd6NxYbQSZ7Yhb
MD5:	84E4A4E3A7031C649A5A72E167090FDB
SHA1:	274383FE065EA8FEFDAE6E3741B000AC788794EE
SHA-256:	6CEC54ADCCA1E191F1BBDECCA1CC1785F252ECA08F7C7D1C21C8EDE0F81E293A
SHA-512:	DDF3378A387E0B58F78BB7C2AD1E0A593E1E85B88662022E96A562DFFC85F1682BBF96AAF72380E580FD6CF84CD252BB59785454F41254BCE492A3BB1D6496C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x6e70d2e6,0x01d6fafa</date><accdate>0x6e70d2e6,0x01d6fafa</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>0x6e70d2e6,0x01d6fafa</date><accdate>0x6e70d2e6,0x01d6fafa</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):	5.039639869981508
Encrypted:	false
SSDEEP:	12:TMHdNMNxcA8vnWimI002EtM3MHdNMNxcA8vnWimI00OYGVEtMb:2d6Nxt8vSZHKd6Nxt8vSZ7Ykb
MD5:	F29C0BAC63B614AC1051E01068286F0E
SHA1:	292925677A624C3CC6DEA88C8FA230540B716E9E
SHA-256:	F32594988A2FB78533A66E3955EDAD97A9E96F57F3FCF237ABEB5687BFB87AAA
SHA-512:	23EC099A45468C1CD6D9B3F30EAB6E9D45DCE351823FE5F8A15A0AAD486F780653D141407A9D15637637CED047C25C736A95365C448D19BA6FEEF443B77527A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x6e6e70ab,0x01d6fafa</date><accdate>0x6e6e70ab,0x01d6fafa</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>0x6e6e70ab,0x01d6fafa</date><accdate>0x6e6e70ab,0x01d6fafa</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):	5.026846375437838
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnA8vnWimI002EtM3MHdNMNxfnA8vnWimI00OYGe5EtMb:2d6NxI8vSZHKd6NxI8vSZ7YLjb
MD5:	852C1A5972999C603B2CE58F6EB31888
SHA1:	79CC25BC789BE4439CB15BD3789A68AEAB143FBA
SHA-256:	8912F9A1A82493D3BD49B43573C93D1BC75689FB19A1926CCC1D35C548493087
SHA-512:	42A9BF9C352D94F65335CA34F0AB93B16984AE30ACDB7F88355AABC8A56F9A1482D4CFFEA8C2B7052A0365F76FB9B4CE93B4D8CB0713854D8AB495E692493198
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x6e6e70ab,0x01d6fafa</date><accdate>0x6e6e70ab,0x01d6fafa</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>0x6e6e70ab,0x01d6fafa</date><accdate>0x6e6e70ab,0x01d6fafa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\NKX81T6F.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):	5.769500647975184
Encrypted:	false
SSDEEP:	12:3R+xnZ7hz8F19o11pv3kqnKYYbtiTnWjkUT0xF4AEdeIQL:3EXzsno3pv3kmKr0qnAjNEkj
MD5:	7475AB6F91FC5B0B2708AD4A73967E03
SHA1:	067403DF45906229A50C8A3E2651AD247D08CACC
SHA-256:	6CCAE6921326D96208DD1044AE3668A52B535620566D920E86EF9F454E36810E
SHA-512:	668D5BF1756C50BCEEEB9DD5D2E3B19F1DE7B23A644D515F1C5FD7F878ED365F683BA412C697C41459B52222A4F32DEFF6FCDCECC8905BA2867E3C772E3DFAD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19.protected-forms.com/XZG5KMmRrbFJla1Z0UjNaRk5VRnRSek0zZFRJMVFXcHdRamxCVm05U01qSTNVMHhvS3pCd2VXYzJiMjlKU0RKV2VUSnpaSGhZUWl0SWFGaE5TRTlyT0dGeGJGVXpOME5HVEcxMk9DOXZNVFk1SzJnMFEwaHBhRUlyUWs5UFVuUlpRMVJhTjBsVFRFczJlVTVwYm1WRWRrWlJZVlJ0VDBZM1dXZ3dXVmd5Y0hBM1pTOVJPVkF4VVc0eWJtTnZibk50WkdSTmRESllPRFV2TlZadlJDOHJaRXcyYUhVNVdrTXhXRlJCUFMwdE5HUmpkMUpVVGs1WE9WUXdZMjQyWmxBd1MwZHVkejA5LS00NjA2MjUyNDMxYTNlYmY0ZmIyOTgxY2NjZGM0MjQzMjk2MzUwNDdm
Preview:	<html>. <head>. <script>window.location.href = 'https://secured-login.net/pages/bdb02071cf5b/XZG5KMmRrbFJla1Z0UjNaRk5VRnRSek0zZFRJMVFXcHdRamxCVm05U01qSTNVMHhvS3pCd2VXYzJiMjlKU0RKV2VUSnpaSGhZUWl0SWFGaE5TRTlyT0dGeGJGVXpOME5HVEcxMk9DOXZNVFk1SzJnMFEwaHBhRUlyUWs5UFVuUlpRMVJhTjBsVFRFczJlVTVwYm1WRWRrWlJZVlJ0VDBZM1dXZ3dXVmd5Y0hBM1pTOVJPVkF4VVc0eWJtTnZibk50WkdSTmRESllPRFV2TlZadlJDOHJaRXcyYUhVNVdrTXhXRlJCUFMwdE5HUmpkMUpVVGs1WE9WUXdZMjQyWmxBd1MwZHVkejA5LS00NjA2MjUyNDMxYTNlYmY0ZmIyOTgxY2NjZGM0MjQzMjk2MzUwNDdm'; </script>. </head>. <body>. </body>.</html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\KB4-logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 200 x 75, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	5864
Entropy (8bit):	7.925096866918419
Encrypted:	false
SSDEEP:	96:YRObJZQcSGBG0v6UBnFSai6Xk2kQ6779zVD0nCXYTu4qWeG0a6lS+adxQVwZ5kkt:iO5SGBRBAkelpXY69We5IhdxQVwfkkt
MD5:	20F88CB052864EF047CBF095E46A23B0
SHA1:	5068F0745178BC0C042B6302ED114516981141BD
SHA-256:	65149B7AFD0CCFDEA4CB383944A47825F33B1A80B092ECA6F74CB01F0C186809
SHA-512:	57E78802933898C66F8E2245357883705E732F0686697601C0F3C2C96B9D345BE131DCD4C0118C657C2A55BC397044DBD06456AB68172C3867C4D055B6EC11EF
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\KB4-logo[1].png	
IE Cache URL:	http://https://cdn2.hubspot.net/hubfs/241394/html_file/files/img/KB4-logo.png
Preview:	.PNG........IHDR.......K.....5|......IDATx..].x.E........(...^ ..(.!.....ry.*".*...Q.u.s.ka.(..'....{ ...G.I.9 .#..r....a.GuO..$$...~_f..^].W...N.."@CCC...... ... ...t...........>| ...,D...9........".I.C.R..p..Mi>.<.....E+@0 .....S...V.PpO@.$k..b...B)z.qv.p@.Z..+.v.$qi......Hr...j............v2.D..s!`..3B.e.&..7....H.......|.(R.$.......Z...P.*.....V.j O..6.5... .....X.....5A .h.?.p.V..A..[...._.............$.W....0..k.+.C.Ti..........T7..E..-*. ...a..gu..M....d..d.!m....%.......Q..3.S.h.T.A.2..j@...b.:.^...2..Y.........d..v?..|.7Bl.....8..y...z.... Q.o.x... ....1.. .B.PgmHX..k.....d...4........0.........R.:{1.]....n.B.&.!...^V....d....B............T.U~ ..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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34[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):	4216944
Entropy (8bit):	5.094462231316503
Encrypted:	false
SSDEEP:	49152:Aw4mDiTFyA6TVfMAeuljHmcIkp5W5FHAzJ7CjhB0ZyA9At+zORaseqlyT7cZdTA6:8x
MD5:	DF03A5ADAA40979F1032E4366588C1F4
SHA1:	A496644F6CBBCF8F830CE5AA6B167C91522E7129
SHA-256:	782DDAF037A5555DA2DAB61C05EBCFCD73BB3AAA36C2762D345F5539BDD61D48
SHA-512:	01329B2DF557BDFC79CAC371256B0313D8CEAE69A74BAA0EC7CEEBE47B16B1D31D419B60FAFF0A31476D48AC31F4255D4210D97A8C7EDC78936453CD201C558
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secured-login.net/assets/application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34.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\9026IKNJ\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\9026IKNJ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\modernizr-79e0181ec91aff04bb01d87cba546535ede843f75d19f5c60f66b8dd6546971f[1].js	
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\9026IKNJ\vendor-de3db557be90cd9dc973[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):	373182
Entropy (8bit):	5.298868955527752
Encrypted:	false
SSDEEP:	6144:XczrLhF2HsGtNjvZBHPg96/6F1HL6jcYyfIUY:7sGzL2HLyd
MD5:	05843568167D3AB2E1A7592FE0BD6D1F
SHA1:	1541FAFBE5716BC280414BC9908B0B3A480120AA
SHA-256:	5F2BEEC184848E24D16E9589FCC16B5182DA6C559D36AF518E8A060987CA2D56
SHA-512:	1867EE67AD46F493C1701B6459197C3C7B106F86AD9790E3D722F3467030F9D291FBC769CFA6C38C7F2042B90D09962DB49737856A45F68291A7A328F63773AD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secured-login.net/packs/js/vendor-de3db557be90cd9dc973.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=1137)}([,,,,,,,,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,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\stoplookthink[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 334x406, frames 3
Category:	downloaded
Size (bytes):	26215
Entropy (8bit):	7.9453849905719185
Encrypted:	false
SSDEEP:	768:HUac4ouUhUGBgwj/VrMXV8BYmbydDCAdx:04XUhVxNMXKBYjdndx
MD5:	F8AC39EA88DB7F7B824BA6703458CB8E
SHA1:	5CA66C9C9941A149B4394C90AF81AB82110B14DE
SHA-256:	92A8C576146BC93A8C34BD32348CADEC152B3FE1DF030A358EC88C4F2FD07A34
SHA-512:	80DBEFAAF01EA5B59344ABB2C54C03E933BD4F237539E9E19EFD342725C47788BF08F0831D8D2FC7AE367BB13F34F1B42E8B6A09D362397BCB0EAFB981D4193 A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s3.amazonaws.com/helpimg/landing_pages/images/stoplookthink.jpg
Preview:	......Exif..II*.....Ducky.....P.....Adobe.d.....N..... .....!1Q..A..aq..."2...BRb#r...3...Ss$Cc....4T.t%....5&.7.....!.1AQaq....."2R...Bbr..#.....3..CSc.%5.....?...].P(.....@.P(.....@...q.mg ...i?a;..#y..O.3.....S...3....SK...k.c.8..8g.....T.s.....}....m;p...Vf..y).Oo.....G1rf.....j..v?.k..e..Oy@.....-..r...:....Z&oyu,...b..c..#....8.jQ.I5...4.DC.]..j.g.\..PqC.A...W...z...Uo1v.. j.....w..up{..+W8.+.X....{.i....3..S+...b....vU..XY.[d&|dHGk....m..Z..plW...g..j;xc...Y.s....q.O.Wg.?.m.}.8.|)`b...>t..EG.....8...._t.)WF.L..N9z...\uw.1..+.....@.P(.....@.P(.....@.P(... ..@.P(<...D5Hps..v;=.W....hz=.S1...Lm.y#.&....kE.....;(.....:M.B..t..pH...*r.d,.mE.4.Lv.<....S.3.....T.DrDq

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\PGA2OXVV.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):	3465
Entropy (8bit):	5.456814746037603
Encrypted:	false
SSDEEP:	96:O4XR7CuP7RU/DI/StNOFzj4tkmdvzCzwDo:OIPVUdYYFUkmd6wk
MD5:	F62231E22755316CD6E318A6951A1450
SHA1:	E11C262C920E47FCFC24425231FAD71100EB15E4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\PGA2OXVV.htm	
SHA-256:	A63090D295271F123681F613DBDAD4BBA335B335C65C81F6E6B6AB9125E6D2A2
SHA-512:	2F63FF946A16CB4A18F9DF27B291D1B74FB5AFCBC0C6C9168E14FA2789EFBBFD3499A43AFA7985D6318F840971573B6A487DBB7D195441E29B707D6AE282572
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secured-login.net/pages/bdb02071cf5b/XZG5KMmRrbFJla1Z0UjNaRk5VRnRSek0zZFRJMVFXcHdRamxCVm05U01qSTNVMHhvS3pCd2VXYzJiMjlKU0RKV2VUSnpaSGhZUWl0SWFGaE5TRTlyT0dGeGJGVXpOME5HVEcxMk9DOXZNVFk1SzJnMFEwaHBhRUlyUWs5UFVuUlpRMVJhTjBsVFRFczJlVTVwYm1WRWRrWlJZVlJ0VDBZM1dXZ3dXVmd5Y0hBM1pTOVJPVkF4VVc0eWJtTnZibk50WkdSTmRESllPRFV2TlZadlJDOHJaRXcyYUhVNVdrTXhXRlJCUFMwdE5HUmpkMUpVVGs1WE9WUXdZMjQyWmxBd1MwZHVkejA5LS00NjA2MjUyNDMxYTNlYmY0ZmIyOTgxY2NjZGM0MjQzMjk2MzUwNDdm
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"/>.. <head>. <script src="/assets/application-ae943aec8610a8eb1cb217c05ea40d5860932dc46d4205e70b987b3f81ea9e34.js"></script>. <script src="/packs/js/vendor-de3db557be90cd9dc973.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-8487e36eef1bec74f06631f19fea0aa171c208e2976373cda5bd0a4b9e230903.css" />.. </

C:\Users\user\AppData\Local\Temp\~DF0169F13BD6A5C051.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	47128
Entropy (8bit):	1.2934790875452853
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+19RZILPhRSjhRS3GRSYRS6RSOiRSWRSQRSwRSzRS:kBqoxKAuqR+1bZILPhwh0G9lniZnXc
MD5:	58804F32BAB2A51440BF1336E88DE697
SHA1:	FCD3D4C6B5CE257C2B4E936D7D1D4EF24E24F991
SHA-256:	31EA6A3D284B1757A5A047CB2035247D70989E682491AFD0A36ECA048804F99A
SHA-512:	3B8F72DF4763C44497CFE2DAD879AE1DF79FF600B7B8B7AB1F28F394B9CF72A0F5741372F24D4F7B1942DD599E58A7C343A53A59DB188E1D889F4E562248245F
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF1AC78276BA855B15.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF71DCD61003AFFC85.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4780955657449577
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fR2mF9l8fR2K9lTq2UdNk4DykNkf00hfn/s7:c9lLh9lLh9lIn9lIn9loN9lot9lWf5wm
MD5:	1985C12B1F48FCC709F374A410D38531
SHA1:	CD8D2CCF77F78397BADFD68948EDD9930F6A0223
SHA-256:	985C7A26A85E9B2CE6A919B978F7540E4B4CF7CC32C675B0DD8AEA93067887A3

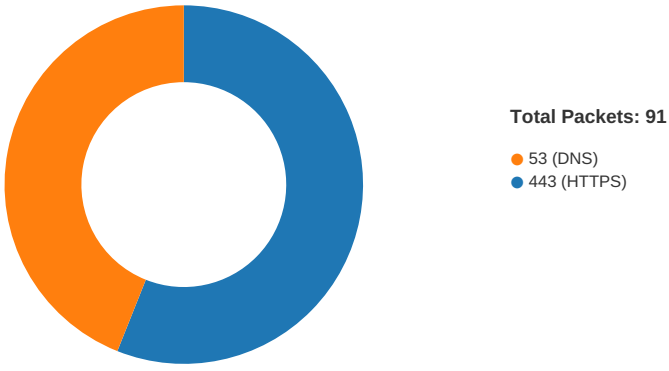
C:\Users\user\AppData\Local\Temp\~DF71DCD61003AFFC85.TMP	
SHA-512:	2ECC6D0C0ED5B9A0252F16B3CC8752C78E2E4690D4F18614D76A8A351F85C4BB28984DFB912B1FC48FF39D673E9DDD15F6A20E48BBEF9B6A33105BD6B51932B
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 4, 2021 14:33:41.175482035 CET	49729	443	192.168.2.4	34.235.194.87
Feb 4, 2021 14:33:41.175606966 CET	49730	443	192.168.2.4	34.235.194.87
Feb 4, 2021 14:33:41.299566984 CET	443	49730	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.299593925 CET	443	49729	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.299736977 CET	49730	443	192.168.2.4	34.235.194.87
Feb 4, 2021 14:33:41.299823046 CET	49729	443	192.168.2.4	34.235.194.87
Feb 4, 2021 14:33:41.311017036 CET	49730	443	192.168.2.4	34.235.194.87
Feb 4, 2021 14:33:41.311094999 CET	49729	443	192.168.2.4	34.235.194.87
Feb 4, 2021 14:33:41.435091972 CET	443	49730	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.435141087 CET	443	49729	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.436234951 CET	443	49730	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.436254025 CET	443	49730	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.436265945 CET	443	49730	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.436279058 CET	443	49730	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.436315060 CET	443	49730	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.436351061 CET	49730	443	192.168.2.4	34.235.194.87
Feb 4, 2021 14:33:41.436430931 CET	49730	443	192.168.2.4	34.235.194.87
Feb 4, 2021 14:33:41.437374115 CET	443	49729	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.437407017 CET	443	49729	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.437423944 CET	443	49729	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.437468052 CET	49729	443	192.168.2.4	34.235.194.87

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 4, 2021 14:33:41.437491894 CET	443	49729	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.437510014 CET	49729	443	192.168.2.4	34.235.194.87
Feb 4, 2021 14:33:41.437517881 CET	443	49729	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.437550068 CET	49729	443	192.168.2.4	34.235.194.87
Feb 4, 2021 14:33:41.437581062 CET	49729	443	192.168.2.4	34.235.194.87
Feb 4, 2021 14:33:41.487876892 CET	49730	443	192.168.2.4	34.235.194.87
Feb 4, 2021 14:33:41.488202095 CET	49729	443	192.168.2.4	34.235.194.87
Feb 4, 2021 14:33:41.497253895 CET	49730	443	192.168.2.4	34.235.194.87
Feb 4, 2021 14:33:41.497447968 CET	49729	443	192.168.2.4	34.235.194.87
Feb 4, 2021 14:33:41.497570992 CET	49730	443	192.168.2.4	34.235.194.87
Feb 4, 2021 14:33:41.614821911 CET	443	49730	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.614841938 CET	443	49730	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.614948034 CET	49730	443	192.168.2.4	34.235.194.87
Feb 4, 2021 14:33:41.614973068 CET	49730	443	192.168.2.4	34.235.194.87
Feb 4, 2021 14:33:41.615346909 CET	443	49729	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.615365028 CET	443	49729	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.615447998 CET	49729	443	192.168.2.4	34.235.194.87
Feb 4, 2021 14:33:41.616611004 CET	49730	443	192.168.2.4	34.235.194.87
Feb 4, 2021 14:33:41.616826057 CET	49729	443	192.168.2.4	34.235.194.87
Feb 4, 2021 14:33:41.624062061 CET	443	49730	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.624196053 CET	49730	443	192.168.2.4	34.235.194.87
Feb 4, 2021 14:33:41.624639034 CET	443	49729	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.624752998 CET	49729	443	192.168.2.4	34.235.194.87
Feb 4, 2021 14:33:41.667958021 CET	443	49730	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.740631104 CET	443	49730	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.784025908 CET	443	49729	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.793921947 CET	443	49730	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.793941021 CET	443	49730	34.235.194.87	192.168.2.4
Feb 4, 2021 14:33:41.794070005 CET	49730	443	192.168.2.4	34.235.194.87
Feb 4, 2021 14:33:42.120074987 CET	49731	443	192.168.2.4	52.203.61.30
Feb 4, 2021 14:33:42.120105982 CET	49732	443	192.168.2.4	52.203.61.30
Feb 4, 2021 14:33:42.243719101 CET	443	49731	52.203.61.30	192.168.2.4
Feb 4, 2021 14:33:42.243815899 CET	49731	443	192.168.2.4	52.203.61.30
Feb 4, 2021 14:33:42.244771957 CET	49731	443	192.168.2.4	52.203.61.30
Feb 4, 2021 14:33:42.247912884 CET	443	49732	52.203.61.30	192.168.2.4
Feb 4, 2021 14:33:42.248033047 CET	49732	443	192.168.2.4	52.203.61.30
Feb 4, 2021 14:33:42.248938084 CET	49732	443	192.168.2.4	52.203.61.30
Feb 4, 2021 14:33:42.368406057 CET	443	49731	52.203.61.30	192.168.2.4
Feb 4, 2021 14:33:42.369427919 CET	443	49731	52.203.61.30	192.168.2.4
Feb 4, 2021 14:33:42.369508028 CET	443	49731	52.203.61.30	192.168.2.4
Feb 4, 2021 14:33:42.369514942 CET	49731	443	192.168.2.4	52.203.61.30
Feb 4, 2021 14:33:42.369545937 CET	443	49731	52.203.61.30	192.168.2.4
Feb 4, 2021 14:33:42.369555950 CET	49731	443	192.168.2.4	52.203.61.30
Feb 4, 2021 14:33:42.369589090 CET	49731	443	192.168.2.4	52.203.61.30
Feb 4, 2021 14:33:42.369632959 CET	443	49731	52.203.61.30	192.168.2.4
Feb 4, 2021 14:33:42.369649887 CET	443	49731	52.203.61.30	192.168.2.4
Feb 4, 2021 14:33:42.369680882 CET	49731	443	192.168.2.4	52.203.61.30
Feb 4, 2021 14:33:42.369712114 CET	49731	443	192.168.2.4	52.203.61.30
Feb 4, 2021 14:33:42.373090029 CET	443	49732	52.203.61.30	192.168.2.4
Feb 4, 2021 14:33:42.374145031 CET	443	49732	52.203.61.30	192.168.2.4
Feb 4, 2021 14:33:42.374193907 CET	443	49732	52.203.61.30	192.168.2.4
Feb 4, 2021 14:33:42.374238014 CET	49732	443	192.168.2.4	52.203.61.30
Feb 4, 2021 14:33:42.374264956 CET	49732	443	192.168.2.4	52.203.61.30
Feb 4, 2021 14:33:42.374269962 CET	443	49732	52.203.61.30	192.168.2.4
Feb 4, 2021 14:33:42.374314070 CET	49732	443	192.168.2.4	52.203.61.30
Feb 4, 2021 14:33:42.374317884 CET	443	49732	52.203.61.30	192.168.2.4
Feb 4, 2021 14:33:42.374361038 CET	49732	443	192.168.2.4	52.203.61.30
Feb 4, 2021 14:33:42.374397039 CET	443	49732	52.203.61.30	192.168.2.4
Feb 4, 2021 14:33:42.374437094 CET	49732	443	192.168.2.4	52.203.61.30
Feb 4, 2021 14:33:42.387963057 CET	49732	443	192.168.2.4	52.203.61.30
Feb 4, 2021 14:33:42.388513088 CET	49732	443	192.168.2.4	52.203.61.30
Feb 4, 2021 14:33:42.388854027 CET	49732	443	192.168.2.4	52.203.61.30
Feb 4, 2021 14:33:42.392450094 CET	49731	443	192.168.2.4	52.203.61.30
Feb 4, 2021 14:33:42.392982006 CET	49731	443	192.168.2.4	52.203.61.30

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 4, 2021 14:33:42.512402058 CET	443	49732	52.203.61.30	192.168.2.4
Feb 4, 2021 14:33:42.512442112 CET	443	49732	52.203.61.30	192.168.2.4
Feb 4, 2021 14:33:42.512547016 CET	443	49732	52.203.61.30	192.168.2.4
Feb 4, 2021 14:33:42.512573957 CET	49732	443	192.168.2.4	52.203.61.30
Feb 4, 2021 14:33:42.512607098 CET	49732	443	192.168.2.4	52.203.61.30
Feb 4, 2021 14:33:42.516377926 CET	443	49731	52.203.61.30	192.168.2.4
Feb 4, 2021 14:33:42.516411066 CET	443	49731	52.203.61.30	192.168.2.4
Feb 4, 2021 14:33:42.516545057 CET	49731	443	192.168.2.4	52.203.61.30
Feb 4, 2021 14:33:42.516572952 CET	443	49731	52.203.61.30	192.168.2.4
Feb 4, 2021 14:33:42.516627073 CET	49731	443	192.168.2.4	52.203.61.30
Feb 4, 2021 14:33:42.554131985 CET	443	49732	52.203.61.30	192.168.2.4
Feb 4, 2021 14:33:42.572026968 CET	443	49732	52.203.61.30	192.168.2.4
Feb 4, 2021 14:33:42.572063923 CET	443	49732	52.203.61.30	192.168.2.4
Feb 4, 2021 14:33:42.572109938 CET	443	49732	52.203.61.30	192.168.2.4
Feb 4, 2021 14:33:42.572153091 CET	49732	443	192.168.2.4	52.203.61.30

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 4, 2021 14:33:39.886601925 CET	49714	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:33:39.942779064 CET	53	49714	8.8.8.8	192.168.2.4
Feb 4, 2021 14:33:41.085809946 CET	58028	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:33:41.161505938 CET	53	58028	8.8.8.8	192.168.2.4
Feb 4, 2021 14:33:42.053231955 CET	53097	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:33:42.117176056 CET	53	53097	8.8.8.8	192.168.2.4
Feb 4, 2021 14:33:42.646687984 CET	49257	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:33:42.691261053 CET	62389	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:33:42.701970100 CET	53	49257	8.8.8.8	192.168.2.4
Feb 4, 2021 14:33:42.736979008 CET	53	62389	8.8.8.8	192.168.2.4
Feb 4, 2021 14:33:46.978369951 CET	49910	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:33:47.043658972 CET	53	49910	8.8.8.8	192.168.2.4
Feb 4, 2021 14:33:48.323175907 CET	55854	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:33:48.370956898 CET	53	55854	8.8.8.8	192.168.2.4
Feb 4, 2021 14:33:49.316037893 CET	64549	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:33:49.372916937 CET	53	64549	8.8.8.8	192.168.2.4
Feb 4, 2021 14:33:50.459434032 CET	63153	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:33:50.508064032 CET	53	63153	8.8.8.8	192.168.2.4
Feb 4, 2021 14:33:51.276690006 CET	52991	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:33:51.325357914 CET	53	52991	8.8.8.8	192.168.2.4
Feb 4, 2021 14:33:52.441620111 CET	53700	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:33:52.492418051 CET	53	53700	8.8.8.8	192.168.2.4
Feb 4, 2021 14:33:57.527975082 CET	51726	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:33:57.573707104 CET	53	51726	8.8.8.8	192.168.2.4
Feb 4, 2021 14:33:57.714395046 CET	56794	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:33:57.768490076 CET	53	56794	8.8.8.8	192.168.2.4
Feb 4, 2021 14:33:58.314773083 CET	56534	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:33:58.363435030 CET	53	56534	8.8.8.8	192.168.2.4
Feb 4, 2021 14:33:59.430830956 CET	56627	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:33:59.476818085 CET	53	56627	8.8.8.8	192.168.2.4
Feb 4, 2021 14:33:59.662559986 CET	56621	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:33:59.708344936 CET	53	56621	8.8.8.8	192.168.2.4
Feb 4, 2021 14:34:00.592724085 CET	63116	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:34:00.640706062 CET	53	63116	8.8.8.8	192.168.2.4
Feb 4, 2021 14:34:01.734743118 CET	64078	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:34:01.789848089 CET	53	64078	8.8.8.8	192.168.2.4
Feb 4, 2021 14:34:02.839287996 CET	64801	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:34:02.893537998 CET	53	64801	8.8.8.8	192.168.2.4
Feb 4, 2021 14:34:03.788042068 CET	61721	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:34:03.833755016 CET	53	61721	8.8.8.8	192.168.2.4
Feb 4, 2021 14:34:05.459888935 CET	51255	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:34:05.506453991 CET	53	51255	8.8.8.8	192.168.2.4
Feb 4, 2021 14:34:05.918134928 CET	61522	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:34:05.977504015 CET	53	61522	8.8.8.8	192.168.2.4
Feb 4, 2021 14:34:08.301451921 CET	52337	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 4, 2021 14:34:08.349836111 CET	53	52337	8.8.8.8	192.168.2.4
Feb 4, 2021 14:34:09.522028923 CET	55046	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:34:09.570646048 CET	53	55046	8.8.8.8	192.168.2.4
Feb 4, 2021 14:34:09.887907982 CET	49612	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:34:09.933636904 CET	53	49612	8.8.8.8	192.168.2.4
Feb 4, 2021 14:34:10.397198915 CET	49285	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:34:10.455549002 CET	53	49285	8.8.8.8	192.168.2.4
Feb 4, 2021 14:34:10.672614098 CET	50601	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:34:10.721864939 CET	53	50601	8.8.8.8	192.168.2.4
Feb 4, 2021 14:34:10.886639118 CET	49612	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:34:10.933573961 CET	53	49612	8.8.8.8	192.168.2.4
Feb 4, 2021 14:34:11.211750031 CET	60875	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:34:11.259954929 CET	53	60875	8.8.8.8	192.168.2.4
Feb 4, 2021 14:34:11.681190014 CET	50601	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:34:11.733175993 CET	53	50601	8.8.8.8	192.168.2.4
Feb 4, 2021 14:34:11.900077105 CET	49612	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:34:11.949590921 CET	53	49612	8.8.8.8	192.168.2.4
Feb 4, 2021 14:34:11.995961905 CET	56448	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:34:12.045865059 CET	53	56448	8.8.8.8	192.168.2.4
Feb 4, 2021 14:34:12.681422949 CET	50601	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:34:12.732556105 CET	53	50601	8.8.8.8	192.168.2.4
Feb 4, 2021 14:34:13.915872097 CET	49612	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:34:13.969794989 CET	53	49612	8.8.8.8	192.168.2.4
Feb 4, 2021 14:34:14.901408911 CET	50601	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:34:14.951153040 CET	53	50601	8.8.8.8	192.168.2.4
Feb 4, 2021 14:34:17.932204962 CET	49612	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:34:17.978598118 CET	53	49612	8.8.8.8	192.168.2.4
Feb 4, 2021 14:34:18.900727034 CET	50601	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:34:18.949353933 CET	53	50601	8.8.8.8	192.168.2.4
Feb 4, 2021 14:34:24.253422976 CET	59172	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:34:24.320907116 CET	53	59172	8.8.8.8	192.168.2.4
Feb 4, 2021 14:34:24.830319881 CET	62420	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:34:24.889302015 CET	53	62420	8.8.8.8	192.168.2.4
Feb 4, 2021 14:34:24.971807003 CET	60579	53	192.168.2.4	8.8.8.8
Feb 4, 2021 14:34:25.044033051 CET	53	60579	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 4, 2021 14:33:41.085809946 CET	192.168.2.4	8.8.8.8	0x562d	Standard query (0)	covid19.protected-forms.com	A (IP address)	IN (0x0001)
Feb 4, 2021 14:33:42.053231955 CET	192.168.2.4	8.8.8.8	0x2130	Standard query (0)	secured-login.net	A (IP address)	IN (0x0001)
Feb 4, 2021 14:33:42.646687984 CET	192.168.2.4	8.8.8.8	0x8937	Standard query (0)	cdn2.hubspot.net	A (IP address)	IN (0x0001)
Feb 4, 2021 14:33:42.691261053 CET	192.168.2.4	8.8.8.8	0xaa02	Standard query (0)	s3.amazonaws.com	A (IP address)	IN (0x0001)
Feb 4, 2021 14:33:57.714395046 CET	192.168.2.4	8.8.8.8	0x3aa2	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
Feb 4, 2021 14:33:41.161505938 CET	8.8.8.8	192.168.2.4	0x562d	No error (0)	covid19.protected-forms.com	landing.training.knowbe4.com		CNAME (Canonical name)	IN (0x0001)
Feb 4, 2021 14:33:41.161505938 CET	8.8.8.8	192.168.2.4	0x562d	No error (0)	landing.training.knowbe4.com		34.235.194.87	A (IP address)	IN (0x0001)
Feb 4, 2021 14:33:41.161505938 CET	8.8.8.8	192.168.2.4	0x562d	No error (0)	landing.training.knowbe4.com		52.203.61.30	A (IP address)	IN (0x0001)
Feb 4, 2021 14:33:41.161505938 CET	8.8.8.8	192.168.2.4	0x562d	No error (0)	landing.training.knowbe4.com		34.202.111.162	A (IP address)	IN (0x0001)
Feb 4, 2021 14:33:41.161505938 CET	8.8.8.8	192.168.2.4	0x562d	No error (0)	landing.training.knowbe4.com		34.237.112.134	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 4, 2021 14:33:41.161505938 CET	8.8.8.8	192.168.2.4	0x562d	No error (0)	landing.training.knowbe4.com		35.153.111.16	A (IP address)	IN (0x0001)
Feb 4, 2021 14:33:41.161505938 CET	8.8.8.8	192.168.2.4	0x562d	No error (0)	landing.training.knowbe4.com		52.202.213.179	A (IP address)	IN (0x0001)
Feb 4, 2021 14:33:42.117176056 CET	8.8.8.8	192.168.2.4	0x2130	No error (0)	secured-login.net		52.203.61.30	A (IP address)	IN (0x0001)
Feb 4, 2021 14:33:42.117176056 CET	8.8.8.8	192.168.2.4	0x2130	No error (0)	secured-login.net		34.235.194.87	A (IP address)	IN (0x0001)
Feb 4, 2021 14:33:42.117176056 CET	8.8.8.8	192.168.2.4	0x2130	No error (0)	secured-login.net		34.202.111.162	A (IP address)	IN (0x0001)
Feb 4, 2021 14:33:42.117176056 CET	8.8.8.8	192.168.2.4	0x2130	No error (0)	secured-login.net		34.237.112.134	A (IP address)	IN (0x0001)
Feb 4, 2021 14:33:42.117176056 CET	8.8.8.8	192.168.2.4	0x2130	No error (0)	secured-login.net		52.202.213.179	A (IP address)	IN (0x0001)
Feb 4, 2021 14:33:42.117176056 CET	8.8.8.8	192.168.2.4	0x2130	No error (0)	secured-login.net		35.153.111.16	A (IP address)	IN (0x0001)
Feb 4, 2021 14:33:42.701970100 CET	8.8.8.8	192.168.2.4	0x8937	No error (0)	cdn2.hubspot.net		104.17.240.204	A (IP address)	IN (0x0001)
Feb 4, 2021 14:33:42.701970100 CET	8.8.8.8	192.168.2.4	0x8937	No error (0)	cdn2.hubspot.net		104.17.243.204	A (IP address)	IN (0x0001)
Feb 4, 2021 14:33:42.701970100 CET	8.8.8.8	192.168.2.4	0x8937	No error (0)	cdn2.hubspot.net		104.17.241.204	A (IP address)	IN (0x0001)
Feb 4, 2021 14:33:42.701970100 CET	8.8.8.8	192.168.2.4	0x8937	No error (0)	cdn2.hubspot.net		104.17.242.204	A (IP address)	IN (0x0001)
Feb 4, 2021 14:33:42.701970100 CET	8.8.8.8	192.168.2.4	0x8937	No error (0)	cdn2.hubspot.net		104.17.244.204	A (IP address)	IN (0x0001)
Feb 4, 2021 14:33:42.736979008 CET	8.8.8.8	192.168.2.4	0xaa02	No error (0)	s3.amazonaws.com		52.216.170.5	A (IP address)	IN (0x0001)
Feb 4, 2021 14:33:57.768490076 CET	8.8.8.8	192.168.2.4	0x3aa2	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
Feb 4, 2021 14:33:41.436315060 CET	34.235.194.87	443	192.168.2.4	49730	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	Tue Jul 07 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	Sat Aug 07 14:00:00 CEST 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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		
Feb 4, 2021 14:33:41.437517881 CET	34.235.194.87	443	192.168.2.4	49729	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	Tue Jul 07 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	Sat Aug 07 14:00:00 CEST 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		
Feb 4, 2021 14:33:42.369632959 CET	52.203.61.30	443	192.168.2.4	49731	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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		
Feb 4, 2021 14:33:42.374317884 CET	52.203.61.30	443	192.168.2.4	49732	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		
Feb 4, 2021 14:33:42.803638935 CET	104.17.240.204	443	192.168.2.4	49734	CN=hubspot.net, 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	Fri Jul 03 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Sat Jul 03 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Feb 4, 2021 14:33:42.804296017 CET	104.17.240.204	443	192.168.2.4	49733	CN=hubspot.net, 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	Fri Jul 03 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Sat Jul 03 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Feb 4, 2021 14:33:43.002944946 CET	52.216.170.5	443	192.168.2.4	49736	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

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 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		
Feb 4, 2021 14:33:43.008462906 CET	52.216.170.5	443	192.168.2.4	49735	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 7040 Parent PID: 800

General

Start time:	14:33:39
Start date:	04/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6595d0000
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	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: 7088 Parent PID: 7040

General

Start time:	14:33:40
Start date:	04/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7040 CREDAT:17410 /prefetch:2
Imagebase:	0xd10000
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