ID: 323914
Sample Name:
Final_report_2020.htm_
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 20:59:34
Date: 27/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

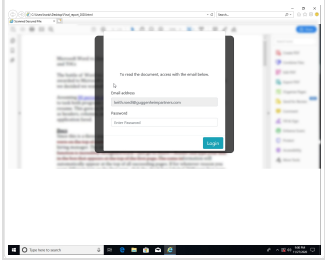
Analysis Report Final_report_2020.htm_

Overview

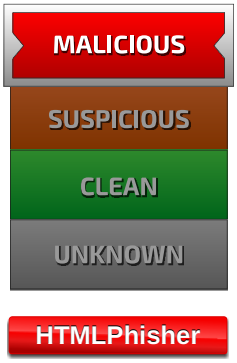
General Information

Sample Name:	Final_report_2020.htm_ (renamed file extension from htm_ to html)
Analysis ID:	323914
MD5:	0c764c478941b7..
SHA1:	81ca3948f11ecf4..
SHA256:	898166e652d7b3..

Most interesting Screenshot:



Detection

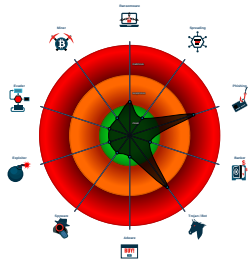


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for doma…
- Yara detected HtmlPhish_7
- Contains strings related to BOT con…
- HTML title does not match URL
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- None HTTPS page querying sensitiv…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 1488 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 2296 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1488 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

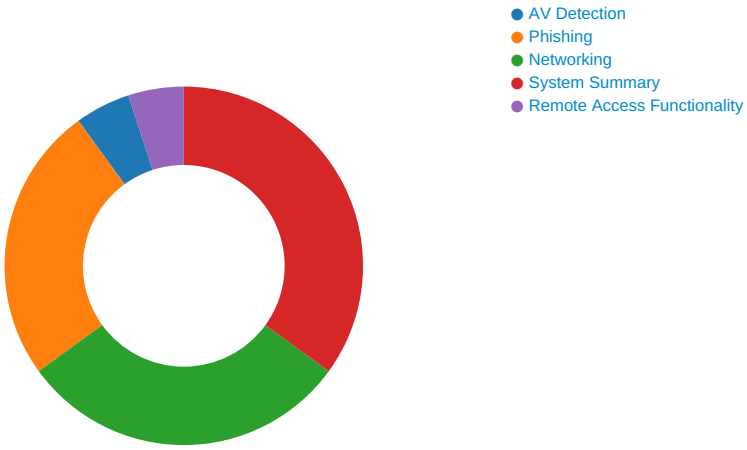
Initial Sample

Source	Rule	Description	Author	Strings
Final_report_2020.html	JoeSecurity_HtmlPhish_7	Yara detected HtmlPhish_7	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

Phishing:

Yara detected HtmlPhish_7

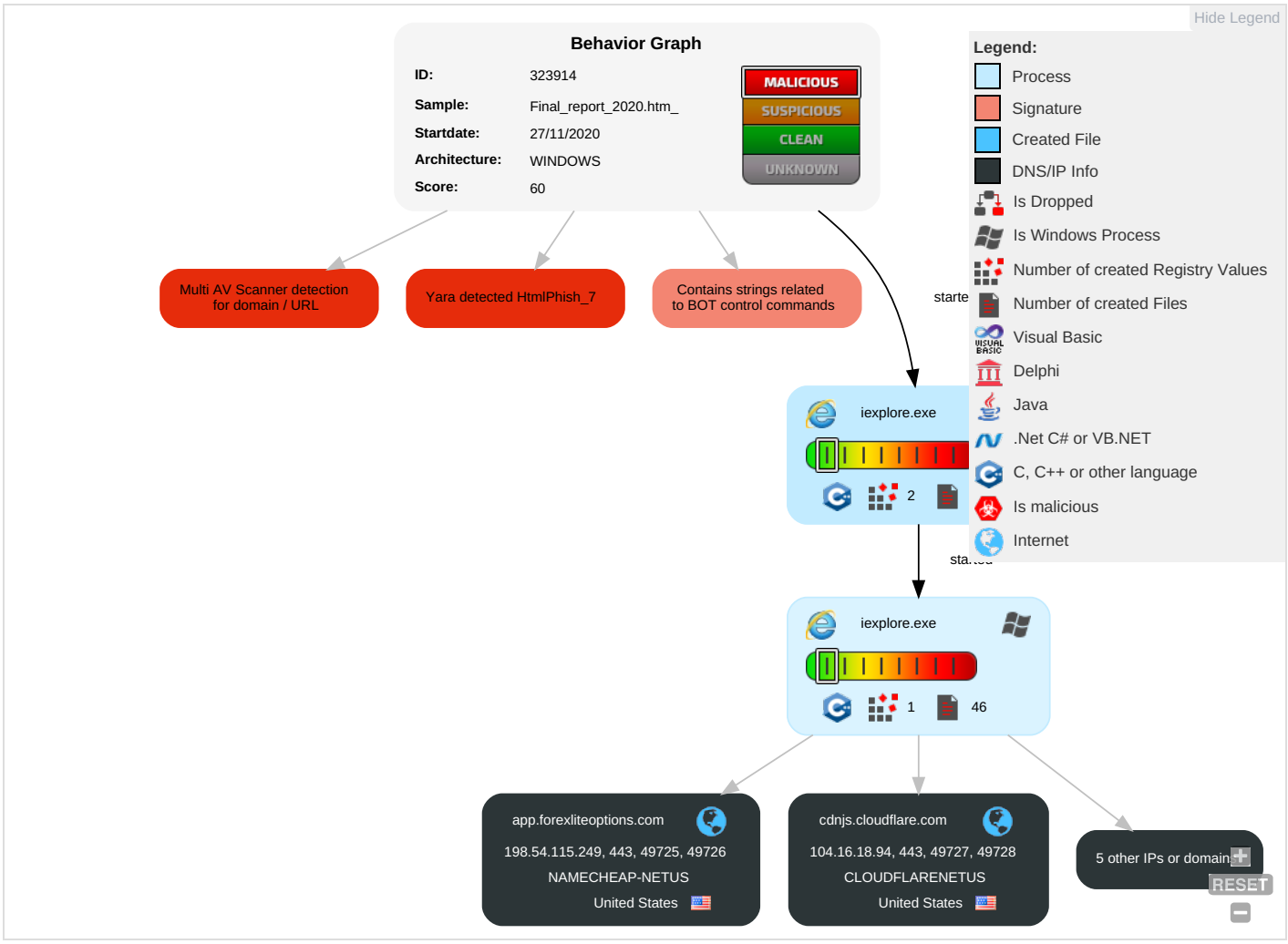
Remote Access Functionality:

Contains strings related to BOT control commands

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

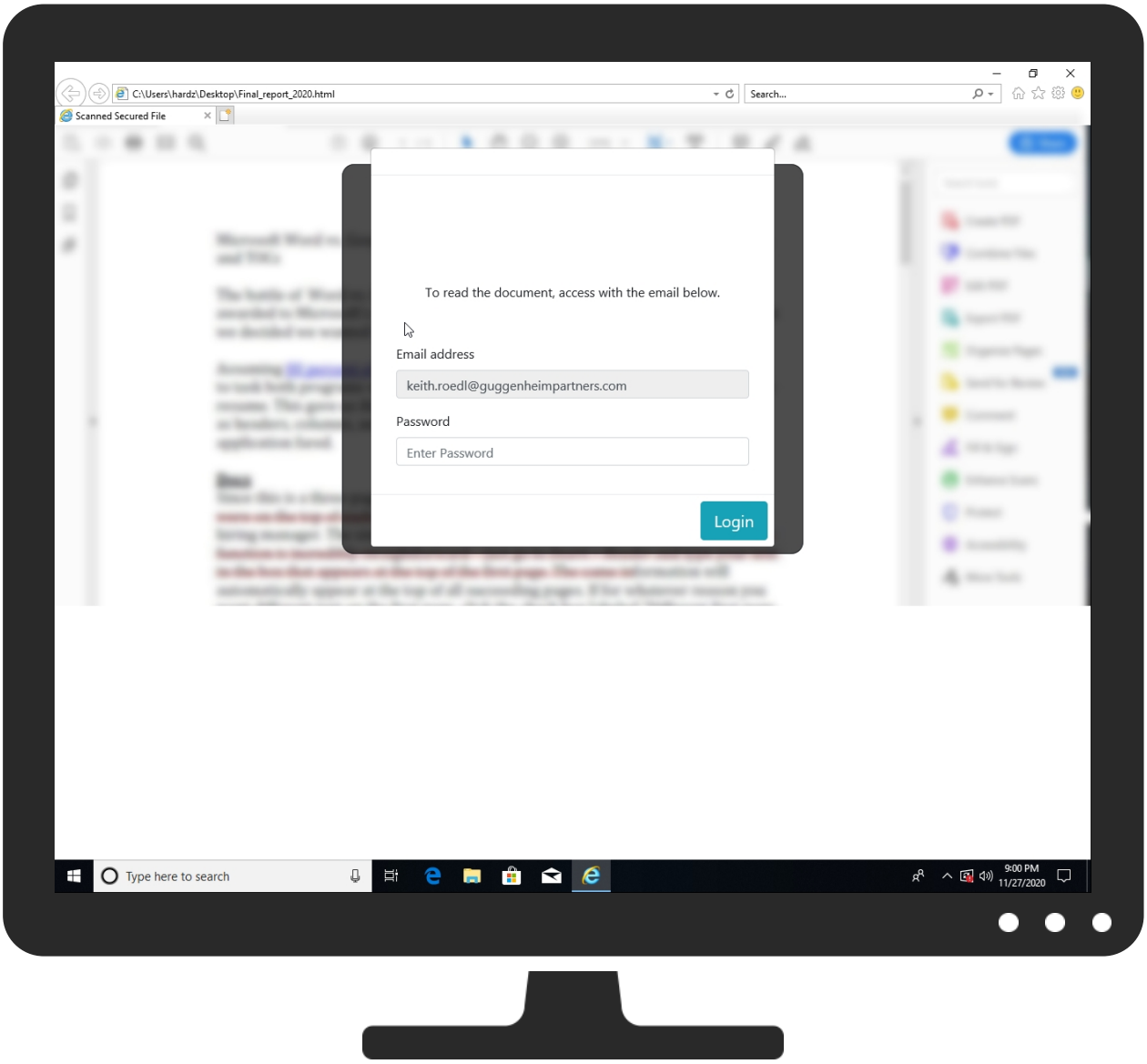
Behavior Graph



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
Final_report_2020.html	2%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
app.forexliteoptions.com	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://app.forexliteoptions.com/core/database/xero/images/8.jpg	6%	Virustotal		Browse
http://https://app.forexliteoptions.com/core/database/xero/images/8.jpg	0%	Avira URL Cloud	safe	
http://ianlunn.github.io/Hover/)	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://ianlunn.github.io/Hover/)	0%	Avira URL Cloud	safe	
http://https://jf-soure.pt/media/viper/send.php	0%	Avira URL Cloud	safe	
http://https://solutionsaec-my.sharepoint.com/:x:/g/personal/jblanquart_solutions-aec_com/Eco5JmDEVEFLtBrJ2	0%	Avira URL Cloud	safe	
http://https://app.forexliteoptions.com/core/database/xero/css/hover.css	0%	Avira URL Cloud	safe	
http://https://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://ianlunn.co.uk/	0%	URL Reputation	safe	
http://ianlunn.co.uk/	0%	URL Reputation	safe	
http://ianlunn.co.uk/	0%	URL Reputation	safe	
http://https://api.statvoo.com/favicon/?url=$	0%	Avira URL Cloud	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdnjs.cloudflare.com	104.16.18.94	true	false		high
app.forexliteoptions.com	198.54.115.249	true	false	• 4%, Virustotal, Browse	unknown
ka-f.fontawesome.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
maxcdn.bootstrapcdn.com	unknown	unknown	false		high

Contacted URLs

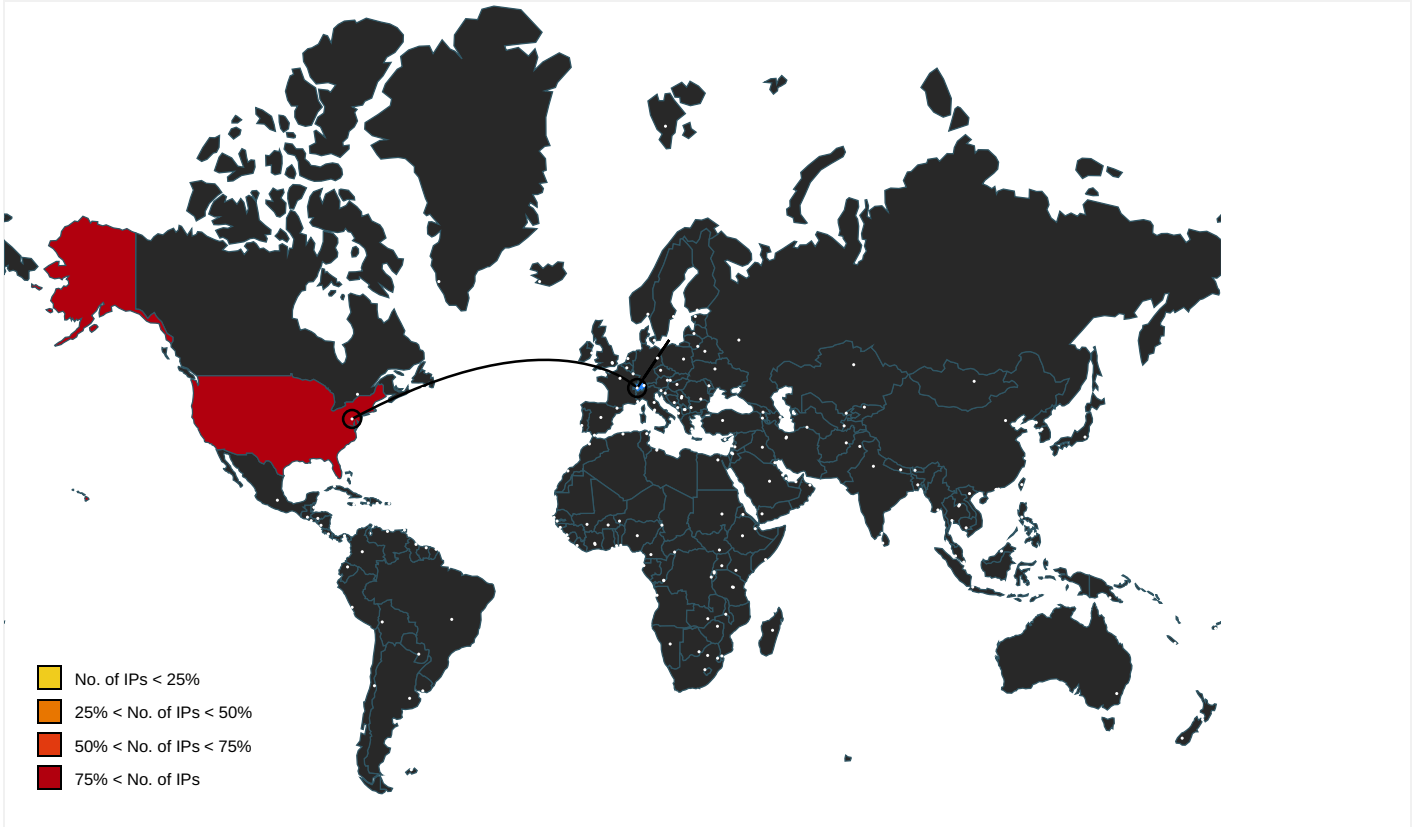
Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/Final_report_2020.html	true		low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://app.forexliteoptions.com/core/database/xero/images/8.jpg	Final_report_2020.html	true	• 6%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://ianlunn.github.io/Hover/)	hover[1].css.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://https://ka-f.fontawesome.com	585b051251[1].js.2.dr	false		high
http://https://code.jquery.com/jquery-3.2.1.slim.min.js	Final_report_2020.html	false		high
http://https://outlook.office.com/mail/inbox	Final_report_2020.html	false		high
http://https://code.jquery.com/jquery-3.1.1.min.js	Final_report_2020.html	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/crypto-js/4.0.0/core.min.js	Final_report_2020.html	false		high
http://www.amazon.com/	msapplication.xml.1.dr	false		high
http://https://jf-soure.pt/media/viper/send.php	Final_report_2020.html	false	• Avira URL Cloud: safe	unknown
http://https://solutionsaec-my.sharepoint.com/:x:/g/personal/jblanquart_solutions-aec_com/Eco5JmDEVEFLtBrJ2	Final_report_2020.html	false	• Avira URL Cloud: safe	unknown
http://www.twitter.com/	msapplication.xml5.1.dr	false		high
http://https://code.jquery.com/jquery-3.3.1.js	Final_report_2020.html	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css	Final_report_2020.html	false		high
http://https://fontawesome.com/license/free	free.min[1].css.2.dr	false		high
http://https://fontawesome.com	free.min[1].css.2.dr	false		high
http://https://github.com/twbs/bootstrap/graphs/contributors)	bootstrap.min[1].js.2.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js	Final_report_2020.html	false		high
http://https://app.forexliteoptions.com/core/database/xero/css/hover.css	Final_report_2020.html	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://getbootstrap.com)	bootstrap.min[1].js.2.dr, bootstrap.min[1].css.2.dr	false	• Avira URL Cloud: safe	low
http://www.youtube.com/	msapplication.xml7.1.dr	false		high
http://ianlunn.co.uk/	hover[1].css.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[1].js.2.dr, bootstrap.min[1].css.2.dr	false		high
http://https://api.statvoo.com/favicon/?url=$	Final_report_2020.html	false	• Avira URL Cloud: safe	unknown
http://www.wikipedia.com/	msapplication.xml6.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/IanLunn/Hover	hover[1].css.2.dr	false		high
http://www.live.com/	msapplication.xml2.1.dr	false		high
http://opensource.org/licenses/MIT).	popper.min[1].js.2.dr	false		high
http://https://kit.fontawesome.com/585b051251.js	Final_report_2020.html	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js	Final_report_2020.html	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/crypto-js/3.1.9-1/md5.js	Final_report_2020.html	false		high
http://www.reddit.com/	msapplication.xml4.1.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.115.249	unknown	United States		22612	NAMECHEAP-NETUS	false
104.16.18.94	unknown	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323914
Start date:	27.11.2020
Start time:	20:59:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Final_report_2020.htm_ (renamed file extension from htm_ to html)
Cookbook file name:	defaultwindowshtmlcookbook.jbs
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:	30
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 • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.phis.troj.winHTML@3/29@6/3
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 104.108.39.131, 209.197.3.24, 172.217.168.10, 209.197.3.15, 216.58.215.234, 104.18.22.52, 104.18.23.52, 172.64.203.28, 172.64.202.28, 51.132.208.181, 23.57.80.111, 152.199.19.161, 2.20.142.209, 2.20.142.210, 92.122.213.247, 92.122.213.194, 51.104.144.132, 20.54.26.129, 92.122.145.220, 51.104.139.180 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, cds.s5x3j6q5.hwcdn.net, arc.msn.com.nsatc.net, ka-f.fontawesome.com.cdn.cloudflare.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, kit.fontawesome.com.cdn.cloudflare.net, fonts.googleapis.com, fs.microsoft.com, ajax.googleapis.com, ie9comview.vo.msecnd.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cds.j3z9t3p6.hwcdn.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.115.249	ATT59829.htm	Get hash	malicious	Browse	
	ATT96626.htm	Get hash	malicious	Browse	
	#U260e#Ufe0fFinal Closing Reports.htm	Get hash	malicious	Browse	
	#Ud83d#Udcdevmshares_msgs-Rexmessagesp_.htm	Get hash	malicious	Browse	
	#U260e#Ufe0fRedreceipt_eltter69-msg-received0100.htm	Get hash	malicious	Browse	
	#U260e#Ufe0fvm__7890671(678-msgs-received01100.htm	Get hash	malicious	Browse	
	#U260e#Ufe0fvmsahres__43029812(89201__-mssgss-8934251.html	Get hash	malicious	Browse	
	#U260e#Ufe0fvmsahres__43029812(89201---mssgss-8934251.htm	Get hash	malicious	Browse	
	Fsc836mx11067098.htm	Get hash	malicious	Browse	
	scan396fx06384866.htm	Get hash	malicious	Browse	
	scan256fx47891482.htm	Get hash	malicious	Browse	
	scan564fx26838194.htm	Get hash	malicious	Browse	
	scan705fx56969208 (002).htm	Get hash	malicious	Browse	
	scan203fx69442412.htm	Get hash	malicious	Browse	
	scan259fx72491224.htm	Get hash	malicious	Browse	
	File-2S0HX7RDF0.html	Get hash	malicious	Browse	
	File-2S0HX7RDF0.html	Get hash	malicious	Browse	
	Scanned-file93050321.htm	Get hash	malicious	Browse	
	Scanned-file36446047.htm	Get hash	malicious	Browse	
	tnfChtUHY2.htm	Get hash	malicious	Browse	
104.16.18.94	http://https://bit.ly/2Gwx0iC	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bit.ly/3jDHDOo	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://Kardanan.com	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/datamaps/0.5.8/datamaps.all.js

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
app.forexliteoptions.com	ATT59829.htm	Get hash	malicious	Browse	• 198.54.115.249
	ATT96626.htm	Get hash	malicious	Browse	• 198.54.115.249
	#U260e#Ufe0fFinal Closing Reports.htm	Get hash	malicious	Browse	• 198.54.115.249
	#Ud83d#Udcdevmshares_msgs-Rexmessagesp_.htm	Get hash	malicious	Browse	• 198.54.115.249
	#U260e#Ufe0fRedreceipt_eltter69-msg-received0100.htm	Get hash	malicious	Browse	• 198.54.115.249
	#U260e#Ufe0fvm__7890671(678-msgs-received01100.htm	Get hash	malicious	Browse	• 198.54.115.249
	#U260e#Ufe0fvmsahres__43029812(89201__-mssgss-8934251.html	Get hash	malicious	Browse	• 198.54.115.249
	#U260e#Ufe0fvmsahres__43029812(89201---mssgss-8934251.htm	Get hash	malicious	Browse	• 198.54.115.249

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Fsc836mx11067098.htm	Get hash	malicious	Browse	• 198.54.115.249
	scan396fx06384866.htm	Get hash	malicious	Browse	• 198.54.115.249
	scan256fx47891482.htm	Get hash	malicious	Browse	• 198.54.115.249
	scan564fx26838194.htm	Get hash	malicious	Browse	• 198.54.115.249
	scan705fx56969208 (002).htm	Get hash	malicious	Browse	• 198.54.115.249
	scan203fx69442412.htm	Get hash	malicious	Browse	• 198.54.115.249
	scan259fx72491224.htm	Get hash	malicious	Browse	• 198.54.115.249
	File-2S0HX7RDF0.html	Get hash	malicious	Browse	• 198.54.115.249
	File-2S0HX7RDF0.html	Get hash	malicious	Browse	• 198.54.115.249
	Scanned-file93050321.htm	Get hash	malicious	Browse	• 198.54.115.249
	Scanned-file36446047.htm	Get hash	malicious	Browse	• 198.54.115.249
	tnfChtUHY2.htm	Get hash	malicious	Browse	• 198.54.115.249
cdnjs.cloudflare.com	Direct Deposit.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	http://https://is.gd/NLY8Sb	Get hash	malicious	Browse	• 104.16.19.94
	http://https://alldomainverifications.web.app#paulo.horta@gnbga.pt	Get hash	malicious	Browse	• 104.16.19.94
	http://https://34.75.2o2.lol/XYWNc0aW9uPWwNsaWNrJngVybD1ovndHRwnczovL3NleY3wVyZWQtbG9naW4ubmV0nL3BhZ2VzLzQyY2FkNTJhZmU3YSZyZWNpcGllbnRfaWQ9NzM2OTg3ODg4JmNhbXBhaWduX3J1bl9pZD0zOTM3OTcz	Get hash	malicious	Browse	• 104.16.18.94
	http://https://hosting-e899f.web.app/#ba11_go_coa_chf@emfa.pt	Get hash	malicious	Browse	• 104.16.18.94
	PAYMENT RECEIPT.html	Get hash	malicious	Browse	• 104.16.19.94
	http://https://sugar-stirring-mockingbird.glitch.me/#comp@hansi.at	Get hash	malicious	Browse	• 104.16.18.94
	http://searchlf.com	Get hash	malicious	Browse	• 104.16.18.94
	http://https://tenderdocsrfp.typeform.com/to/RVzhstxV	Get hash	malicious	Browse	• 104.16.18.94
	http://bit.ly/33hfhnG	Get hash	malicious	Browse	• 104.16.19.94
	http://https://www.canva.com/design/DAEOiuhLwDM/BOj9WYGqioxJf6uGii9b8Q/view?utm_content=DAEOiuhLwDM&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 104.16.18.94
	http://https://omgzone.co.uk/	Get hash	malicious	Browse	• 104.16.19.94
	ATT59829.htm	Get hash	malicious	Browse	• 104.16.19.94
	http://email.balluun.com/ls/click?upn=KzNQqcw6vAwizrX-2Fig1Ls6Y5D9N6j9I5FZfBCN8B2wRxBmpXcbUQvKOFUzJGiw-2F3Qy64T8VZ2LXT8NNNJG9bemh7vjcLDgF5-2FXPBBBqdJ0-2BpvIlXlKrZECAirL9YySN2b1LT-2Bcy1l-2F0fp1Pwvv3l4j7XHHKagv-2FxlVdd85P38ZuA-2Bvv5JF3QaAOx19sqG0-2BnULpm_J-2BsRItFMcwpTA18DVdBlGBJyUhFuIaAEybVNgKjH795y-2Bjn2esAEGPPa76dl-2BxD62wo4xT0BtNrFdVu0eWgx-2F6eRqupI7yZWQAa-2FBr1dlsLgX0hlcDSdDmAHsaZaG3WUUyADLR7thqFcU32Djt0AEfQ9qS0428-2BH1u-2Fk1E3KVFo9lePxc9mOWOHzwBkFv-2FOdeNUShdwqtjGBw2zuSNSTyLDRcypBOMpUtPdiR8ihMQ0-3D	Get hash	malicious	Browse	• 104.16.18.94
	http://https://elementalhospitality-my.sharepoint.com/:o:/g/personal/damian_elementaleu_com/EpbQzbjzWKlHjcvPXBBiFIMBOCLQJZggMYJcpD4357rxtQ?e=Vhznra	Get hash	malicious	Browse	• 104.16.19.94
	http://HTTPS://WWW.SSLLABS.COM/SSLTEST/VIEWMYCLIENT.HTML	Get hash	malicious	Browse	• 104.16.19.94
	http://https://lowhormonebooster.com/Win/index.php	Get hash	malicious	Browse	• 104.16.19.94
	http://https://mshad4064.typeform.com/to/TEgIyNGg	Get hash	malicious	Browse	• 104.16.18.94
	http://https://cts.indeed.com/v0?tk=1df9t5skc2g3980p&r=%68%74%74%70%73%3a%2f%2f%61%6e%61%6c%79%74%69%63%73%2e%74%77%69%74%74%65%72%2e%63%6f%6d%2f%64%61%61%2f%30%2f%64%61%61%5f%6f%70%74%6f%75%74%5f%61%63%74%69%6f%6e%73%3f%61%63%74%69%6f%6e%5f%69%64%3d%33%26%70%61%72%74%69%63%69%70%61%6e%74%5f%69%64%3d%37%31%36%26%72%64%3d%68%74%74%70%73%3a%2f%2f%66%72%61%31%2e%64%69%67%69%74%61%6c%6f%63%65%61%6e%73%70%61%63%65%73%2e%63%6f%6d%2f%73%32%32%2f%69%6e%64%65%78%2e%68%74%6d%6c%3f#matthias.kirsch@iti.org	Get hash	malicious	Browse	• 104.16.18.94

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	norit.dll	Get hash	malicious	Browse	• 104.31.69.174
	380000_USD_INV_011740_NOV_2020.jar	Get hash	malicious	Browse	• 104.20.22.46
	380000_USD_INV_011740_NOV_2020.jar	Get hash	malicious	Browse	• 104.20.23.46
	http://https://tinyurl.com/y9xs2oe6	Get hash	malicious	Browse	• 104.20.138.65
	case.2522.xls	Get hash	malicious	Browse	• 104.31.87.113
	http://https://ch1.amorozon.fr/.zz?&78387439&user=jon.parr@syngenta.com	Get hash	malicious	Browse	• 104.27.129.197
	case.2522.xls	Get hash	malicious	Browse	• 104.31.87.113
	coinomi-1.20.0.apk	Get hash	malicious	Browse	• 162.159.200.1
	Purchase Order.exe	Get hash	malicious	Browse	• 172.67.143.180
	http://fonts.mafia-server.net	Get hash	malicious	Browse	• 104.18.40.210
	caw.exe	Get hash	malicious	Browse	• 162.159.138.232
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	http://https://is.gd/NLY8Sb	Get hash	malicious	Browse	• 104.16.19.94
	Soda_PDF_12_Installer (7).exe	Get hash	malicious	Browse	• 104.16.181.79
	REQUEST FOR BID 26-11-2020.ppt	Get hash	malicious	Browse	• 104.18.49.20
	http://https://alldomainverifications.web.app#paulo.horta@gnbga.pt	Get hash	malicious	Browse	• 104.16.19.94
	DHL_Nov 2020 at 1.85_8BZ290_PDF.jar	Get hash	malicious	Browse	• 104.20.23.46
	DHL_Nov 2020 at 1.85_8BZ290_PDF.jar	Get hash	malicious	Browse	• 104.20.23.46
	http://https://erabansoupala.blogspot.com//?m=0	Get hash	malicious	Browse	• 172.67.194.249
NAMECHEAP-NETUS	http://https://soportesdchilers.gtfkfg.online	Get hash	malicious	Browse	• 198.54.116.217
	caw.exe	Get hash	malicious	Browse	• 199.188.200.123
	Vm2120896.htm	Get hash	malicious	Browse	• 198.54.117.244
	dO0yHANE0T.exe	Get hash	malicious	Browse	• 198.54.115.130
	PO_0012009.xlsx	Get hash	malicious	Browse	• 198.54.122.60
	PT300975-inv.exe	Get hash	malicious	Browse	• 198.54.117.244
	PR24869408-V2.PDF.exe	Get hash	malicious	Browse	• 198.54.122.60
	http://https://dhumketubd.com/DifferenceCard/login.php	Get hash	malicious	Browse	• 198.54.117.200
	vnaSKDMnLG.dll	Get hash	malicious	Browse	• 63.250.47.200
	ATT59829.htm	Get hash	malicious	Browse	• 198.54.115.249
	PO EME39134.xlsx	Get hash	malicious	Browse	• 63.250.38.18
	http://https://www.ebhadhara.com/ova/office365/YWp1bm5hcmthckBrcm9sbGJvbmRyYXRpbmdzLmNvbQ0%3D	Get hash	malicious	Browse	• 199.192.28.206
	FxzOwcXb7x.exe	Get hash	malicious	Browse	• 198.54.122.60
	7OKYiP6gHy.exe	Get hash	malicious	Browse	• 198.54.117.217
	ptFlhqUe89.exe	Get hash	malicious	Browse	• 63.250.38.18
	Yarranton.co.uk.htm	Get hash	malicious	Browse	• 199.188.200.218
	PO#010-240.exe	Get hash	malicious	Browse	• 162.213.255.53
	PO_010-240.exe	Get hash	malicious	Browse	• 162.213.255.53
	EME.39134.xlsx	Get hash	malicious	Browse	• 63.250.38.18
	http://omivjsyyqzyxfria.riantscapital.com/kampo/anNhY2tldHRAYWR2ZW50aXN0aGVhbHRoY2FyZS5jb20=	Get hash	malicious	Browse	• 198.54.120.245

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	norit.dll	Get hash	malicious	Browse	• 104.16.18.94 • 198.54.115.249
	http://https://tinyurl.com/y9xs2oe6	Get hash	malicious	Browse	• 104.16.18.94 • 198.54.115.249
	http://https://ch1.amorozon.fr/.zz?&78387439&user=jon.parr@syngenta.com	Get hash	malicious	Browse	• 104.16.18.94 • 198.54.115.249
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 104.16.18.94 • 198.54.115.249
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 104.16.18.94 • 198.54.115.249
	http://https://ib.adnxs.com/getuid?https://a.adrsp.net/dsp/ci/2/E8quIp-RUbrsO6XnZMkW-Z82IQ_D_mG3bKHPbyWqDJNAFkp2JZBiBD4qwJcECqeCBYZccMP3y2IGKpMkBSJ3emkLIw/%24UID	Get hash	malicious	Browse	• 104.16.18.94 • 198.54.115.249
	http://fonts.mafia-server.net	Get hash	malicious	Browse	• 104.16.18.94 • 198.54.115.249

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 104.16.18.94 • 198.54.115.249
	INV-FATURA010009.xlsx	Get hash	malicious	Browse	• 104.16.18.94 • 198.54.115.249
	INV-FATURA010009.xlsx	Get hash	malicious	Browse	• 104.16.18.94 • 198.54.115.249
	http://https://alldomainverifications.web.app#paulo.horta@gnbga.pt	Get hash	malicious	Browse	• 104.16.18.94 • 198.54.115.249
	http://https://broughtguarantees.com/1/oZrheD/cHBlcmluaUBhZmZpbmlvbmdyb3VwLmNvbQ%3D%3D&d=DwMDaQ	Get hash	malicious	Browse	• 104.16.18.94 • 198.54.115.249
	http://https://offiubtj7banjz48zrg8d4nz2ns9.web.app/?c=brynjar.t.gudmundsson@landsbanki.is	Get hash	malicious	Browse	• 104.16.18.94 • 198.54.115.249
	http://https://erabansoupala.blogspot.com//?m=0	Get hash	malicious	Browse	• 104.16.18.94 • 198.54.115.249
	http://https://mincast.us-south.cf.appdomain.cloud/redirect/?email=prampon@soteb.fr	Get hash	malicious	Browse	• 104.16.18.94 • 198.54.115.249
	http://https://dagevleri.com/inv	Get hash	malicious	Browse	• 104.16.18.94 • 198.54.115.249
	http://https://dealmaker.pl/au_au.html	Get hash	malicious	Browse	• 104.16.18.94 • 198.54.115.249
	http://https://wilkinsonbutler.tallverse.ga/YW1iZXJAd2lsa2luc29uYnV0bGVyLmNvbQ==	Get hash	malicious	Browse	• 104.16.18.94 • 198.54.115.249
	http://https://wilkinsonbutler.tallverse.ga/YW1iZXJAd2lsa2luc29uYnV0bGVyLmNvbQ==	Get hash	malicious	Browse	• 104.16.18.94 • 198.54.115.249
	http://https://34.75.2o2.lol/XYWNc0aW9uPWwNsaWNrJngVybD1ovndHRwnczovL3NleY3wVyZWQtbG9naW4ubmV0nL3BhZ2VzLzQyY2FkNTJhZmU3YSZyZWNpcGllbnRfaWQ9NzM2OTg3ODg4JmNhbXBhaWduX3J1bl9pZD0zOTM3OTcz	Get hash	malicious	Browse	• 104.16.18.94 • 198.54.115.249

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{9D350949-3136-11EB-90E4-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8501393748557728
Encrypted:	false
SSDEEP:	96:rhZyZN2p9WU2tUufUFtMUqUnfUnZfUnNMX:rhZyZN2p9WntjfitMpMgfeMX
MD5:	039DF364F0D070E81973E98407504544
SHA1:	4A3DB568EA8E4D8D11360720DDF028505811CCFA
SHA-256:	8000DE7408BD4CA2B1E81AFBCB2F3A8C492416CCC5D3D4852C4CD816114AEC0D
SHA-512:	0760EB75DA1AC9BE52335C3444CD770DBA754864F83C6ECBA3BF1E14492D8278B26BCB457FA1364FE20FCA1FD4935FEDB6518E24188768D7958347431A573678
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\{9D35094B-3136-11EB-90E4-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28384
Entropy (8bit):	1.9411010353756109
Encrypted:	false
SSDEEP:	192:rhZSQdz6T3kXFjR2IkWbMJYjnrIn+pzeMkAMkJMkVbEGr:rn/dWT0XhAMIJmEKKMFMEMO9
MD5:	4EB6629E12504618DBA64594F031CF9B

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9D35094B-3136-11EB-90E4-ECF4BB862DED}.dat	
SHA1:	EF7FB0F2D5AE21B1AF39DF345FC880DF87D9F04B
SHA-256:	8720A082DE7016476743E2DAF48622F1A5AD98A826FFF212C95F183EE4C62D1E
SHA-512:	13D3C31B19B24EDA673720AC0C1D10ED0DE0135DD4E9D73AAEE3AE70026232FC4FAA10C0E53FDDB2185349E18AACFFCD982981A58A776AE3FA09230FE46BE E42
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\{9D35094C-3136-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5664937453914625
Encrypted:	false
SSDEEP:	48:IwlGcprAGwpaeG4pQSGrapbS2rGQpKAG7HpRhsTGIpG:r7ZIQe6UBS2FAbTh4A
MD5:	67D6736B23C8C3B714A128C4B514525E
SHA1:	2CAC0BDB6E10D53A361905A941437A98EF453AEE
SHA-256:	11F84F00B7B88924DF7ACBDC8626A176F8402EBDDB1543DBEB071EABE2500CE8
SHA-512:	E526728BC38FA61B2648CC57B2ECB9B92AE3BC3EE7AF50782E68E57C620DE0C7F5FEE68AF75D40440387EA45512C7BEC029A700F7BDE14E4090360981F814CD D
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):	5.127927212603229
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEzsQnWimI002EtM3MHdNMNxOEzsQnWimI00ObVbkEtMb:2d6NxOQSZHKd6NxOQSZ76b
MD5:	FE98AC6ACE8069CF5953B916FCD1C1F7
SHA1:	19D2B4B4625EE4D7A70F8608651E4D86E7E58733
SHA-256:	2F11AE2284EC1D41EBCD1050CB93707145DB6D85A196B31E2DB8760EC7079706
SHA-512:	F21317D0902A455797266D9ED33B6FE53BF0DCAC14DF9F5FAB4DE23901F168C45B46426234300125DE7B3B81B2B5E46094696B24493327002B2BCA6A41A9D079
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x72bc8d5b,0x01d6c543</date>< accdate>0x72bc8d5b,0x01d6c543</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>0x72bc8d5b,0x01d6c543</date><accdate>0 x72bc8d5b,0x01d6c543</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):	5.166575650903079
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2knoMnWimI002EtM3MHdNMNxe2knoMnWimI00Obkak6EtMb:2d6NxrKoMSZHKd6NxrKoMSZ7Aa7b
MD5:	A1FCABBC7F9D0CCE96F35077296BC3F8
SHA1:	0DD3B7A6A73C1AECC17EDA9321866EA790B6FCC6
SHA-256:	A631B6FEC48AF72A6A0F305EC8A4F6679D41A697783F7011DEEF34FB1CFAEF04
SHA-512:	A7B74E21F0785524EA6FC4F0C4EB504A851283D8B1B7974E7CEE685C0B31CFB5F280D968AFB61AD4D60CF947CEA0C38CB8DFA1CE46A403BCDC63FC69D6471 77
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x72b56643,0x01d6c543</date><accdate>0x72b56643,0x01d6c543</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>0x72b56643,0x01d6c543</date><accdate>0x72b56643,0x01d6c543</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.146345332175874
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLzsQnWimI002EtM3MHdNMNxvLzsQnWimI00ObmZEtMb:2d6NxvpSZHKd6NxvpSZ7mb
MD5:	D48AE1923DE1C87373FEC438A336B763
SHA1:	83C28F4C7BE1B52870F0B9516A8A1DB44EAACD6E
SHA-256:	A63BB78A6824CB99FF2DF71BFD1486DF448C67E5C1A5A8517A944BDDFC34923E
SHA-512:	2680EE73B78416A631691BA3D3857667ADB07FA1E5A2AE4EC9F0ACD8F86BE329FCF0B613475F492DCAE1B2172467454C53A3D85D9A723E2AAA6ABC39E0CFDEC7
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x72bc8d5b,0x01d6c543</date><accdate>0x72bc8d5b,0x01d6c543</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>0x72bc8d5b,0x01d6c543</date><accdate>0x72bc8d5b,0x01d6c543</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.127361546568971
Encrypted:	false
SSDEEP:	12:TMHdNMNxiIBOB1nWimI002EtM3MHdNMNxiIBOB1nWimI00Obd5EtMb:2d6NxhIbSZHKd6NxhIbSZ7Jjb
MD5:	B72C947926902F29A1C98A8A78D88A3B
SHA1:	801233466AC3B1AA4C118D16213B0B12C0859F99
SHA-256:	9522CFA7EEC06EE508F8C2DF0FBDDA005FADBFA35C0D153E3558139ED808BC7E
SHA-512:	12A3D9D03F0560BED2C786F8442F5BC207731D62EE44F346E263E43806FCEAF2DBE2CD4535AFC15A23B0B7FC5B93C19A6E12F8D3E59315EC33A6D69830BF0367
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x72ba2aff,0x01d6c543</date><accdate>0x72ba2aff,0x01d6c543</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>0x72ba2aff,0x01d6c543</date><accdate>0x72ba2aff,0x01d6c543</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.133282124707956
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwCd7dSnWimI002EtM3MHdNMNxhGwCd7dSnWimI00Ob8K075EtMb:2d6NxQxZSSZHKd6NxQxZSSZ7YKajb
MD5:	2286656A3A0D740B68206C4A1B8BB229
SHA1:	BFC9EF56BED17FE815A4FCCCF481A223EB540805
SHA-256:	2295F0DB7585551A77C117D72060F66DC355FC28A322BBFD1F9255DDB20EE289
SHA-512:	DC0EF997BC25F4FD980E1543DC30458016E53E466DE02D51AF26A4C59A8BAEB883D91ED2A730C2499B23146502B36ED9B39C03EB2CD4FB49DDCE9DD19F726BB
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x72beefd7,0x01d6c543</date><accdate>0x72beefd7,0x01d6c543</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>0x72beefd7,0x01d6c543</date><accdate>0x72beefd7,0x01d6c543</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):	5.12882010215063
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nzsQnWimI002EtM3MHdNMNx0nzsQnWimI00ObxEtMb:2d6Nx0NSZHKd6Nx0NSZ7nb
MD5:	7C7A95A0B807A978A059480F454D17ED
SHA1:	44D138E977F457170A0BC99FDABC20635E39CD3B
SHA-256:	A05F698B624F78C8D0C46A3E2F06B9D6171C1F50019ADD31D98A87FA7C2EB743
SHA-512:	0219DEE2729622DE6DAE12EC66884F31E0E4F6830EDA982CE3C17D585C332002B270A8871E8AFD40E89A253F4F39004DD560901F9E1AB7C49E9A942DE2F9426
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x72bc8d5b,0x01d6c543</date><accdate>0x72bc8d5b,0x01d6c543</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>0x72bc8d5b,0x01d6c543</date><accdate>0x72bc8d5b,0x01d6c543</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):	5.168350913873925
Encrypted:	false
SSDEEP:	12:TMHdNMNxxzsQnWimI002EtM3MHdNMNxxzsQnWimI00Ob6Kq5EtMb:2d6NxnSZHKd6NxnSZ7ob
MD5:	84B72785F4C86B76E9430B6A3F26A9FE
SHA1:	D9263F8578799C1AAF018628537FE3A0A198B97B
SHA-256:	2AB0B6548EF2C598AB56C1C84B67437C7F57720805E89842B9E11CA6317094C0
SHA-512:	B60309B68B0140F3FB9CB9391B961369347E5608951118DE044C9F836E98C24A3F7F1535E1AAC27812B13E00E1FC7E0A99C7F656DD1D2456F60837176C1C3BE7
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x72bc8d5b,0x01d6c543</date><accdate>0x72bc8d5b,0x01d6c543</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>0x72bc8d5b,0x01d6c543</date><accdate>0x72bc8d5b,0x01d6c543</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):	5.141333026790235
Encrypted:	false
SSDEEP:	12:TMHdNMNxcD4o4SnWimI002EtM3MHdNMNxcD4o4SnWimI00ObVEtMb:2d6NxOSZHKd6NxOSZ7Db
MD5:	24AAD35FDB930D68315FB0F5371A121C
SHA1:	159D17B77083B08A276134110C29E895E7D09ACE
SHA-256:	68B87F16A6BD5848AD86CD69AD49D5050D5F04299D8C96C98E2FAB555C171009
SHA-512:	6BDD78F2D07E20C47D31CF1FD4A73411AE544ED89570174257E0A50835132934B8551DF1CDF9712F9089805055C61F28D6696B9F1E6D101D4D5EB40C87DDF5E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x72b7c8b1,0x01d6c543</date><accdate>0x72b7c8b1,0x01d6c543</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>0x72b7c8b1,0x01d6c543</date><accdate>0x72b7c8b1,0x01d6c543</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):	5.112875913308287
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnIBOB1nWiml002EtM3MHdNMNxfnIBOB1nWiml00Obe5EtMb:2d6NxAlbSZHKd6NxAlbSZ7ijb
MD5:	021FC7995873807AEA8E37AF27E5BA38
SHA1:	9E784AAA0C0CDA8159611742A7D5F7B43EA793EF
SHA-256:	FD813B92F90E3CFE88FF5211270183020F612F605419D30385442A2EF32D52BA
SHA-512:	E82DEE407E568A5B601F8F9455C3FAEFB4ED65423B67E4E4BCE53A5F871D32BA7F04C3EBDF636A70D4D735CB101F93BAFA7EA735A8D01903FE09B2818DB83E91
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x72ba2aff,0x01d6c543</date><accdate>0x72ba2aff,0x01d6c543</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>0x72ba2aff,0x01d6c543</date><accdate>0x72ba2aff,0x01d6c543</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\8[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=12, height=709, bps=0, PhotometricIntepretation=RGB, orientation=upper-left, width=1200], baseline, precision 8, 1200x646, frames 3
Category:	downloaded
Size (bytes):	161118
Entropy (8bit):	7.5594351594508185
Encrypted:	false
SSDEEP:	3072:WucfAcwuKGuN2q/gSsqnk4br5XUGpppLqfmazv7l04J:OMuKbYOF355XEuAv7lnJ
MD5:	F17B5B1163EFB6D2D47DE6BAE6D3A9CD
SHA1:	6D6964B34BC44C6D2B106ADE1AE675985B96D012
SHA-256:	7829F065E0E10C8466F3D57766E0719421B7B652F6A1082F21B98702F1B28A30
SHA-512:	7C0CBEF1D3CAE66A18C74544E593803C2EEC56817E762A385D54437BC7D597B2598886B0C0EDF72C6E934E9F146CEFC89392A492DB5425A1071E61CA1F15685
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://app.forexliteoptions.com/core/database/xero/images/8.jpg
Preview:	.....Exif..MM.*.....(.....1....."....2.....i.....$.....'.....'.Adobe Photoshop CC 2015 (Windows).2020:01:21 13:41:42.....0221.....r.....z.(.....%.....H.....H.....Adobe_CM.....Adobe.d.....V...".....?.....3.....!.1.AQa."q.2....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?.....q..KJG..x.."....]..TX...[^.m...R.....X.5..j?p.A.RI%0...MN.$..@.4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery-3.1.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	86709
Entropy (8bit):	5.367391365596119
Encrypted:	false
SSDEEP:	1536:9NhEyjjTikEJO4edXXe9J578go6MWXqcVhrLyB4Lw13sh2bzrl1+iuH7U3gBORDT:jxcq0hrLZwpsYbmzORDU8Cu5
MD5:	E071ABDA8FE61194711CFC2AB99FE104
SHA1:	F647A6D37DC4CA055CED3CF64BBC1F490070ACBA
SHA-256:	85556761A8800D14CED8FCD41A6B8B26BF012D44A318866C0D81A62092EFD9BF
SHA-512:	53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D6906765
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://code.jquery.com/jquery-3.1.1.min.js
Preview:	/*! jQuery v3.1.1 | (c) jQuery Foundation | jquery.org/license */.!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.1.1",r=function(a,b){return new r.fn.init(a,b)},s=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,t=/^-ms-/,u=/-([a-z])/g,v=function(a,b){return b.toUpperCase()};r.fn=r.prototype={jquery:q,constructor:r,length:0,toArray:function(){return f.call(this)},get:function(a){return null==a?f.call(this):a<0?this[a+this.length]:this[a]},pushStack:function(a){var b=r.merge(this.con

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery-3.2.1.slim.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery-3.2.1.slim.min[1].js	
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	69597
Entropy (8bit):	5.369216080582935
Encrypted:	false
SSDEEP:	1536:qNhEyjjTikEJO4edXXe9J578go6MWX2xkjVe4c4j2ll2Ac7pK3F71QDU8CuT:Exc2yjq4j2uYnQDU8CuT
MD5:	5F48FC77CAC90C4778FA24EC9C57F37D
SHA1:	9E89D1515BC4C371B86F4CB1002FD8E377C1829F
SHA-256:	9365920887B11B33A3DC4BA28A0F93951F200341263E3B9CEFD384798E4BE398
SHA-512:	CAB8C4AFA1D8E3A8B7856EE29AE92566D44CEEAD70C8D533F2C98A976D77D0E1D314719B5C6A473789D8C6B21EBB4B89A6B0EC2E1C9C618FB1437EBC77D3A269
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://code.jquery.com/jquery-3.2.1.slim.min.js
Preview:	/*! jQuery v3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_evalUrl,-event/ajax,-effects,-effects/Tween,-effects/animatedSelector | (c) JS Foundation and other contributors | jquery.org/license */!function(a,b){"use strict";"object"==typeof module &&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	144877
Entropy (8bit):	5.049937202697915
Encrypted:	false
SSDEEP:	1536:GcoqwrUPyDHU7c7TcDEBi82NcuSELL4d/+oENM6HN26Q:VoPgPard2oENM6HN26Q
MD5:	450FC463B8B1A349DF717056FBB3E078
SHA1:	895125A4522A3B10EE7ADA06EE6503587CBF95C5
SHA-256:	2C0F3DCFE93D7E380C290FE4AB838ED8CADFF1596D62697F5444BE460D1F876D
SHA-512:	93BF1ED5F6D8B34F53413A86EFD4A925D578C97ABC757EA871F3F46F340745E4126C48219D2E8040713605B64A9ECF7AD986AA8102F5EA5ECF9228801D962F5D
Malicious:	false
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css
Preview:	/*! * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors. * Copyright 2011-2018 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--orange:#fd7e14;--yellow:#ffc107;--green:#28a745;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--primary:#007bff;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;--warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoint-xl:1200px;--font-family-sans-serif:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol";--font-family-monospace:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monospace}*,::after,::before{box-sizing:border-box}html{font-family:sans

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bootstrap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	48944
Entropy (8bit):	5.272507874206726
Encrypted:	false
SSDEEP:	768:9VG5R15WbHVKZrycEHSYro34CrSLB6WU/6DqBf4l1B:9VIRuo53XiwWTvl1B
MD5:	14D449EB8876FA55E1EF3C2CC52B0C17
SHA1:	A9545831803B1359CFEED47E3B4D6BAE68E40E99
SHA-256:	E7ED36CEEE5450B4243BBC35188AFABDFB4280C7C57597001DE0ED167299B01B
SHA-512:	00D9069B9BD29AD0DAA0503F341D67549CCE28E888E1AFFD1A2A45B64A4C1BC460D81CFC4751857F991F2F4FB3D2572FD97FCA651BA0C2B0255530209B182F2
Malicious:	false
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js
Preview:	/*! * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,n){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function s(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function r(){return(r=Object.assign||function(t){for(var e=1;e<arguments.length;e++){var n=arguments[e];for(var i in n)Object.prototype.hasOwnProperty.call(n,i)&&(t[i]=n[i])}return t}).apply(this,arguments)}e=e&&e.hasOwnProperty("default")?e.default:e,n=n&&n.hasOwnProp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\core.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\core.min[1].js	
Category:	downloaded
Size (bytes):	3891
Entropy (8bit):	5.218566356649445
Encrypted:	false
SSDEEP:	96:+BxNTqS7zkXW4kaT5NoUlyHhf+iLVQH5gwP:+5rkm4kaT5DafpLVu5xP
MD5:	E9325F1AECE67B8282928D85F07DE758
SHA1:	94C8B9CB36019463170593F85569B607B0722DA3
SHA-256:	80D0635FE9783BEC07A43419DEB4E9969BF30A78F008386826C9723B7651F43C
SHA-512:	3D0B1DCC3B613CAB69DB7D2E0FB96E9D3430E82C0D4CF9DDE4B3F77B7FFE69F83D70D92B2FB52C7D65D3DC45B902BF5767949D00370F0D7B3504058D6BD39ED
Malicious:	false
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/crypto-js/4.0.0/core.min.js
Preview:	!function(t,n){"object"==typeof exports?module.exports=exports=n():"function"==typeof define&&define.amd?define([],n):t.CryptoJS=n()}(this,function(){var t=t||function(f){var t;if("undefined"!=typeof window&&window.crypto&&(t=window.crypto),!t&&"undefined"!=typeof window&&window.msCrypto&&(t=window.msCrypto),!t&&"undefined"!=typeof global&&global.crypto&&(t=global.crypto),!t&&"function"==typeof require)try{t=require("crypto")}catch(t){}function i(){if(t){if("function"==typeof t.getRandomValues)try{return t.getRandomValues(new Uint32Array(1))[0]}catch(t){}if("function"==typeof t.randomBytes)try{return t.randomBytes(4).readInt32LE()}catch(t){}}throw new Error("Native crypto module could not be used to get secure random number.")}var e=Object.create||function(t){var n;return r.prototype=t,n=new r,r.prototype=null,n};function r(){}var n={},o=n.lib={},s=o.Base={extend:function(t){var n=e(this);return t&&n.mixIn(t),n.hasOwnProperty("init")&&this.init!==n.init||(n.init=function(){n.$super.ini

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	85578
Entropy (8bit):	5.366055229017455
Encrypted:	false
SSDEEP:	1536:EYE1JVoiB9JqZdXXe2pD3PgoIiulrUndZ6a4tfOR7WpfWBZ2BJda4w9W3qG9a986:v4J+OlfOhWppCW6G9a98Hr2
MD5:	2F6B11A7E914718E0290410E85366FE9
SHA1:	69BB69E25CA7D5EF0935317584E6153F3FD9A88C
SHA-256:	05B85D96F41FFF14D8F608DAD03AB71E2C1017C2DA0914D7C59291BAD7A54F8E
SHA-512:	0D40BCCAA59FEDECF7243D63B33C42592541D0330FEFC78EC81A4C6B9689922D5B211011CA4BE23AE22621CCE4C658F52A1552C92D7AC3615241EB640F8514B
Malicious:	false
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js
Preview:	/*! jQuery v2.2.4 | (c) jQuery Foundation | jquery.org/license */!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="2.2.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,function(b,c){return a.call

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\md5[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	9418
Entropy (8bit):	4.463752957660408
Encrypted:	false
SSDEEP:	192:w0T6FUnMrjD6YnySWnfr98bi+0G/S6k8jqElWY7:w0bMrjD6GySWfr98bi+0G6UYM
MD5:	349498F298A6E6E6A85789D637E89109
SHA1:	E626C530154C07527ABCFB1F83B9EC578A81B234
SHA-256:	97DC67431DBD3360EA838FECAD611A30F540F8389BBD15B89A1E14BA8DBB54AA
SHA-512:	89360B3D300EED66778657553CB9E9B957584E42C5356CB270FD15E124E1FE1C31495A7583702A8EA2D9CBC504DF841D653E98417AD4E51E6416815070E927FA
Malicious:	false
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/crypto-js/3.1.9-1/md5.js
Preview:	;(function (root, factory) {..if (typeof exports === "object") {.../// CommonJS...module.exports = exports = factory(require("./core"));..}..else if (typeof define === "function" && define.amd) {.../// AMD...define(["./core"], factory);..}..else {.../// Global (browser)...factory(root.CryptoJS);..}.}(this, function (CryptoJS) {...(function (Math) {.. // Shortcuts.. var C = CryptoJS;.. var C_lib = C.lib;.. var WordArray = C_lib.WordArray;.. var Hasher = C_lib.Hasher;.. var C_algo = C.algo;... // Constants table.. var T = [];... // Compute constants.. (function () {.. for (var i = 0; i < 64; i++) {.. T[i] = (Math.abs(Math.sin(i + 1)) * 0x100000000) | 0;.. }.. }());... /**.. * MD5 hash algorithm... */.. var MD5 = C_algo.MD5 = Hasher.extend({.. _doReset: function () {.. this._hash = new WordArray.init([.. 0x67452301, 0xefcdab89,.. 0x98badcfe, 0x10325476..]);..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\popper.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	19188

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\popper.min[1].js	
Entropy (8bit):	5.212814407014048
Encrypted:	false
SSDEEP:	384:+CbuG4xGNoDic2UjKPafxwC5b/4xQviOJU7QzxzivDdE3pcGdjkd/9jt3B+Kb964:zb4xGmiJfaf7gxQvVU7eziv+cSjknZ3f
MD5:	70D3FDA195602FE8B75E0097EED74DDE
SHA1:	C3B977AA4B8DFB69D651E07015031D385DED964B
SHA-256:	A52F7AA54D7BCAAFA056EE0A050262DFC5694AE28DEE8B4CAC3429AF37FF0D66
SHA-512:	51AFFB5A8CFD2F93B473007F6987B19A0A1A0FB970DDD59EF45BD77A355D82ABBBD60468837A09823496411E797F05B1F962AE93C725ED4C00D514BA40269D1
Malicious:	false
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js
Preview:	/*. Copyright (C) Federico Zivolo 2017. Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT).. */(function(e,t){'object'==typeof exports&&'undefined'!=typeof module?module.exports=t():'function'==typeof define&&define.amd?define(t):e.Popper=t()})(this,function(){'use strict';function e(e){return e&&'[object Function]'==={}.toString.call(e)}function t(e,t){if(1!==e.nodeType)return[];var o=getComputedStyle(e,null);return t?o[t]:o}function o(e){return'HTML'===e.nodeName?e:e.parentNode||e.host}function n(e){if(!e)return document.body;switch(e.nodeName){case'HTML':case'BODY':return e.ownerDocument.body;case'#document':return e.body;}var i=t(e),r=i.overflow,p=i.overflowX,s=i.overflowY;return /(auto|scroll)/.test(r+s+p)?e:n(o(e))}function r(e){var o=e&&e.offsetParent,i=o&&o.nodeName;return i&&'BODY'!==i&&'HTML'!==i?-1!==['TD','TABLE'].indexOf(o.nodeName)&&'static'===t(o,'position')?r(o):o:e?e.ownerDocument.documentElement:document.documentElement}functio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\free-v4-shims.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	26701
Entropy (8bit):	4.829785000026929
Encrypted:	false
SSDEEP:	192:bP6hT1bIl4w0QUmQ10PwKLaAu5CwWavpHo4O6wgLPbJVR8XD7mycP:Ohal4w0QK+PwK05eavpmgPPeXD7mycP
MD5:	2E4C3DA4EAE1C876A281D6CA5A7A5B4C
SHA1:	92AD084AAB53B7AA8C761CD66BDFB1F79B9CAED7
SHA-256:	CFFF9EA502195A7B96FE38DECA9188A59B758DEEECC2CD4E78AEA7D911E638C6
SHA-512:	F324F308649F47E3C25BF021C1776A4326750D04D9392B7F200331E806514B69E7579FB23D7B2107A3B30CB96926554C0DE13F45FD1397BDAE89938DD52A7EBF
Malicious:	false
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.1/css/free-v4-shims.min.css
Preview:	/*!. * Font Awesome Free 5.15.1 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.fa.fa-glass:before{content:"\f000"}.fa.fa-meetup{font-family:"Font Awesome 5 Brands";font-weight:400}.fa.fa-star-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-star-o:before{content:"\f005"}.fa.fa-close:before,.fa.fa-remove:before{content:"\f00d"}.fa.fa-gear:before{content:"\f013"}.fa.fa-trash-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-trash-o:before{content:"\f2ed"}.fa.fa-file-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-file-o:before{content:"\f15b"}.fa.fa-clock-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-clock-o:before{content:"\f017"}.fa.fa-arrow-circle-o-down{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arrow-circle-o-down:before{content:"\f358"}.fa.fa-arrow-circle-o-up{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arro

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\free.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	60351
Entropy (8bit):	4.728636008010348
Encrypted:	false
SSDEEP:	768:OUh31IPiyXNq4YxBowbgJlkwF//zMQyYJYX9Bft6VSz8:OU0PxXE4YXJgndFTfy9lt5Q
MD5:	319D424BA89A84BBD230A3B5F7024193
SHA1:	1AE1807CDED8F2E41D2541BCCA8E0D7077FBA6F4
SHA-256:	4F02BD6F018D6F08C37C39F2D114101BEAC342C2C065046635E5ED0C42853590
SHA-512:	A68CAB17CCD1C4DDEAD9124B75CF0CF0C12C4E914902AECE79DCC4C42167B58B565467F20F72C48DFA85490F1895F89F074C85E825D548AD12410741A3302E
Malicious:	false
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.1/css/free.min.css
Preview:	/*!. * Font Awesome Free 5.15.1 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.fa,.fab,.fad,.fal,.far,.fas{-moz-osx-font-smoothing:grayscale;-webkit-font-smoothing:antialiased;display:inline-block;font-style:normal;font-variant:normal;text-rendering:auto;line-height:1}.fa-lg{font-size:1.33333em;line-height:.75em;vertical-align:-.0667em}.fa-xs{font-size:.75em}.fa-sm{font-size:.875em}.fa-1x{font-size:1em}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-6x{font-size:6em}.fa-7x{font-size:7em}.fa-8x{font-size:8em}.fa-9x{font-size:9em}.fa-10x{font-size:10em}.fa-fw{text-align:center;width:1.25em}.fa-ul{list-style-type:none;margin-left:2.5em;padding-left:0}.fa-ul>li{position:relative}.fa-li{left:-2em;position:absolute;text-align:center;width:2em;line-height:inherit}.fa-border{border:.08em solid #eee;border-radius:.1em;padding:.2em .25em .15em}.fa-pul

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\585b051251[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	9972
Entropy (8bit):	5.162816885495512
Encrypted:	false
SSDEEP:	192:VEH6KnRK9ZoshohwIQEEKIMTmlD0yZTwUEhA0jxRjhO3YXyl80YT1rxMn:rxDohl1OrfohwYXyl80YZm

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\585b051251[1].js	
MD5:	BA42298E76E6F714456BF30A3C080955
SHA1:	C4DA8F08824D48D16936871078DCDCEFF875137F
SHA-256:	704E83D712675EF5372B082BC11DCE00C8E498836B383C4514099BA5E0B9F833
SHA-512:	8B4664DCCA234CF61D3D72655252B73FF100E1EE96D2902B3F4E09099AAEC9DDF1AE538642366CC957FDAE5C489AFDECF756BF75A5F89A3D424ED65C139F81C
Malicious:	false
IE Cache URL:	http://https://kit.fontawesome.com/585b051251.js
Preview:	window.FontAwesomeKitConfig = {"asyncLoading":{"enabled":true},"autoA11y":{"enabled":true},"baseUrl":"https://ka-f.fontawesome.com","detectConflictsUntil":null,"iconUploads":{},"license":"free","method":"css","minify":{"enabled":true},"token":"585b051251","v4FontFaceShim":{"enabled":false},"v4shim":{"enabled":true},"version":"5.15.1"};.!function(t){"function"==typeof define&&define.amd?define(t):t()}((function(){"use strict";function t(e){return(t="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(t){return typeof t}:function(t){return t&&"function"==typeof Symbol&&t.constructor===Symbol&&t!==Symbol.prototype?"symbol":typeof t})(e)}function e(t,e,n){return e in t?Object.defineProperty(t,e,{value:n,enumerable:!0,configurable:!0,writable:!0}):t[e]=n,t}function n(t,e){var n=Object.keys(t);if(Object.getOwnPropertySymbols){var o=Object.getOwnPropertySymbols(t);e&&(o=o.filter((function(e){return Object.getOwnPropertyDescriptor(t,e).enumerable}))),n.push.apply(n,o)}return n}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	211
Entropy (8bit):	5.026484232218891
Encrypted:	false
SSDEEP:	6:0IFFwKh+56ZRWHMqh7izlpdBEoKOEEJTONin:jFWmO6ZRoMqt6p3EondOY
MD5:	04F7435B2672FBE66984EA436E7087C6
SHA1:	44896875E69B297EB979CC0D3E8522D872656BA8
SHA-256:	F9088C15A062F0C7708C3864C5E261A2E4961DFEB0F150DF744FAEC2E3B74AD6
SHA-512:	9A1D01A7FAC3D6B205CFA37C05A93AFA9D903D4D35DCB16E31D3A31D19CD65B8DE5D66E626BC7F70D07841C779E20CD2C2DD6254824F96DE0E8E576E156F17D
Malicious:	false
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Yellowtail&display=swap
Preview:	@font-face {. font-family: 'Yellowtail';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/yellowtail/v11/OZpGg_pnoDtINPfRIlLohlvHxw.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\hover[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	114697
Entropy (8bit):	4.9296726009523
Encrypted:	false
SSDEEP:	1536:67O7EesvXIPRX4PT8aZv8qoXIoqbTFaFeTxvyAZ+D7M71D:qXIPRX4PT3
MD5:	FAC4178C15E5A86139C662DAFC809501
SHA1:	EF1481841399156A880EC31B07DDA9CFAA1ACE39
SHA-256:	BB88454962767EB6F2DDB1AABAAF844D8A57DE7E8F848D7F6928F81B54998452
SHA-512:	0902219B6E236FBF9D8173D1D452C8733C1BF67B0EB906CC9866EA0C27C2D08F6DA556D01475E9B54E2C6CE797B230BFBD5F39055CE0C71EA4D3E36872C3789
Malicious:	false
IE Cache URL:	http://https://app.forexliteoptions.com/core/database/xero/css/hover.css
Preview:	/*!. * Hover.css (http://ianlunn.github.io/Hover/). * Version: 2.3.2. * Author: Ian Lunn @IanLunn. * Author URL: http://ianlunn.co.uk/. * Github: https://github.com/IanLunn/Hover.. * Hover.css Copyright Ian Lunn 2017. Generated with Sass.. */./* 2D TRANSITIONS */./* Grow */..hvr-grow {. display: inline-block;. vertical-align: middle;. -webkit-transform: perspective(1px) translateZ(0);. transform: perspective(1px) translateZ(0);. box-shadow: 0 0 1px rgba(0, 0, 0, 0);. -webkit-transition-duration: 0.3s;. transition-duration: 0.3s;. -webkit-transition-property: transform;. transition-property: transform;.}..hvr-grow:hover, .hvr-grow:focus, .hvr-grow:active {. -webkit-transform: scale(1.1);. transform: scale(1.1);.}../* Shrink */..hvr-shrink {. display: inline-block;. vertical-align: middle;. -webkit-transform: perspective(1px) translateZ(0);. transform: perspective(1px) translateZ(0);. box-shadow: 0 0 1px rgba(0, 0, 0, 0);. -webkit-transition-duration: 0.3s;. transition-

C:\Users\user\AppData\Local\Temp\~DF0BDE7E2723C6F460.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	36145
Entropy (8bit):	0.6211034537985556
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+5XF03wn+pzeMkAMkJMkVb:kBqoxKAuqR+5XF03wKKMFMEMO
MD5:	A9CDCD5EE96DF6718A69C27C0D2BD9DF
SHA1:	0B6330AE9913D42C4D376DD587D3D419DCE8A5C4
SHA-256:	0D2758F30C130118BA96D9BC06711D6E5A667E2B10AC860A0E0271D47719F31A
SHA-512:	F910F4E0C0F9301CF21414E82E1FDD4F26134E529A804733F389865AD3099D64E05751093654C0BBDAC0C2AD8A9D83814302FA8768F679C400EC1FD62712EA68

C:\Users\user\AppData\Local\Temp\~DF0BDE7E2723C6F460.TMP	
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF44D9FBA5FF02588F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47979376927188255
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo7F9loB9lWspqLpCVnD:kBqoIKU0qlCVnD
MD5:	3CD3F1C13855AE604F045B7283672887
SHA1:	2C429F60B6CC88FF3ED67B119247C161512050BF
SHA-256:	F181BBAE0E8C56A9A25D3267BD2B482CF6748B4DE135A050BE53044FF8DC031D
SHA-512:	AB27ED69CB00B1E3C6D186B790FCBBE1F343D5092076174F5728DBE972712A3E11687D0DDE41E203E78A6247A6DACA8E37A227390232028E8EBACD204FDE14 9
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF9773F3BBCD74FE8F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	1.2060146634008178
Encrypted:	false
SSDEEP:	96:kBqoxDhHWSVSE+FO/m8LwojM0Jp5I8hYPhJzWPY2Sw3:kBqoxDhHjgE+W8ojM07JihCI
MD5:	8F6C6FD2175EF389086F9EAC8B9AC354
SHA1:	F6C8AF2F9DF694E48C97394F562F5B71B2C74ECF
SHA-256:	359A2DE04E9C6F7B676DBEFBBC53A6E6E5809BCB3AF16A31BA243D231640AB2B
SHA-512:	3FFAFDC1D6EEA06D9F26950DEA17FD267521392614F821BC9F9221C541487AEA242552AC640426F639B0D76BF5F948384DD3F79787817CCD30CF397C8A7ED60
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

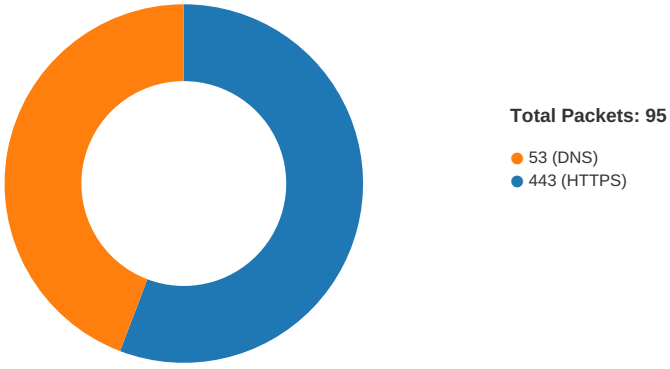
File type:	HTML document, ASCII text, with CRLF line terminators
Entropy (8bit):	4.740540823904859
TrID:	• HyperText Markup Language (12001/1) 20.69% • HyperText Markup Language (12001/1) 20.69% • HyperText Markup Language (11501/1) 19.83% • HyperText Markup Language (11501/1) 19.83% • HyperText Markup Language (11001/1) 18.97%
File name:	Final_report_2020.html
File size:	17073
MD5:	0c764c478941b76371c019b9a1b7c607
SHA1:	81ca3948f11ecf4ffb266b9ef6e95ec708d3d7f1
SHA256:	898166e652d7b302eea1d3436e15fe47375e1bc8e3767a 9f072d2f29adf82958
SHA512:	e6cae65efbd5a7221ff49a6f4adc3633d19216e95a085ec 87abdc53d952d7a33747fd43dceebaa9e00f8879495cb45 3a834aa6ef25dfc6c7b57b8c73bf246c44
SSDEEP:	192:1/VAbPtzo2A2PThJIhwVIhwVIhwVIhwVrBolXkWG UUqR+5qb45:nAb1lhhhoRvk

General

File Content Preview:	<!doctype html>..<html lang="en">....<head>.. <script src="https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>.. <script src="https://code.jquery.com/jquery-3.1.1.min.js">.. <script src="https://code.jquery.com/jquery-3.3.1.js

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 21:00:23.021199942 CET	49725	443	192.168.2.3	198.54.115.249
Nov 27, 2020 21:00:23.022093058 CET	49726	443	192.168.2.3	198.54.115.249
Nov 27, 2020 21:00:23.059129000 CET	49728	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.059148073 CET	49727	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.059223890 CET	49729	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.075509071 CET	443	49729	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.075536966 CET	443	49727	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.075598001 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.075613976 CET	49729	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.075660944 CET	49727	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.075670004 CET	49728	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.088746071 CET	49728	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.089850903 CET	49727	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.095046997 CET	49729	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.105283976 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.106288910 CET	443	49727	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.107188940 CET	443	49727	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.107230902 CET	443	49727	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.107398987 CET	49727	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.107449055 CET	49727	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.108820915 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.108863115 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.108920097 CET	49728	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.108954906 CET	49728	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.111402035 CET	443	49729	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.112788916 CET	443	49729	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.112839937 CET	443	49729	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.112927914 CET	49729	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.112977028 CET	49729	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.174876928 CET	49728	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.175266027 CET	49728	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.175396919 CET	49728	443	192.168.2.3	104.16.18.94

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 21:00:23.175463915 CET	49728	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.175533056 CET	49728	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.175739050 CET	49727	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.176074028 CET	49727	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.178793907 CET	49729	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.179601908 CET	49729	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.191277027 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.191590071 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.191620111 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.191652060 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.191762924 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.192004919 CET	443	49727	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.192210913 CET	443	49725	198.54.115.249	192.168.2.3
Nov 27, 2020 21:00:23.192286968 CET	443	49727	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.192316055 CET	49725	443	192.168.2.3	198.54.115.249
Nov 27, 2020 21:00:23.192429066 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.192498922 CET	49728	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.192600012 CET	443	49726	198.54.115.249	192.168.2.3
Nov 27, 2020 21:00:23.192742109 CET	49726	443	192.168.2.3	198.54.115.249
Nov 27, 2020 21:00:23.193227053 CET	49725	443	192.168.2.3	198.54.115.249
Nov 27, 2020 21:00:23.193381071 CET	443	49727	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.193445921 CET	443	49727	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.193490982 CET	49727	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.193509102 CET	49727	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.194468975 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.194605112 CET	49728	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.194672108 CET	49728	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.195009947 CET	443	49729	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.195287943 CET	443	49729	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.195369959 CET	443	49729	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.195426941 CET	49729	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.195476055 CET	49729	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.195772886 CET	443	49729	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.195804119 CET	443	49729	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.195883036 CET	49729	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.197876930 CET	49727	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.198496103 CET	49729	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.198719978 CET	49726	443	192.168.2.3	198.54.115.249
Nov 27, 2020 21:00:23.204466105 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.204495907 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.204534054 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.204561949 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.204566002 CET	49728	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.204588890 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.204606056 CET	49728	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.204654932 CET	49728	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.204911947 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.204941988 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.204977989 CET	49728	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.204981089 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.205018044 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.205018997 CET	49728	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.205030918 CET	49728	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.205060005 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.205073118 CET	49728	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.205097914 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.205113888 CET	49728	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.205127001 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.205152035 CET	49728	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.205168009 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.205173969 CET	49728	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.205199003 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.205224037 CET	49728	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.205260992 CET	49728	443	192.168.2.3	104.16.18.94

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 21:00:23.206562996 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.206588984 CET	443	49728	104.16.18.94	192.168.2.3
Nov 27, 2020 21:00:23.206617117 CET	49728	443	192.168.2.3	104.16.18.94
Nov 27, 2020 21:00:23.206621885 CET	443	49728	104.16.18.94	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 21:00:16.412625074 CET	63492	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:16.439886093 CET	53	63492	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:17.225233078 CET	60831	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:17.261343956 CET	53	60831	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:18.053812981 CET	60100	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:18.081268072 CET	53	60100	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:18.945116043 CET	53195	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:18.972121954 CET	53	53195	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:20.199929953 CET	50141	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:20.227188110 CET	53	50141	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:21.006670952 CET	53023	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:21.033824921 CET	53	53023	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:21.783248901 CET	49563	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:21.820782900 CET	53	49563	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:22.114197969 CET	51352	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:22.141371012 CET	53	51352	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:22.889672995 CET	59349	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:22.889955044 CET	57084	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:22.910965919 CET	58823	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:22.916913986 CET	53	57084	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:22.930038929 CET	57568	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:22.933468103 CET	53	59349	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:22.938219070 CET	53	58823	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:22.967278957 CET	50540	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:22.972989082 CET	54366	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:22.973576069 CET	53	57568	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:22.994182110 CET	53	50540	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:23.003499985 CET	53034	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:23.019804001 CET	53	54366	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:23.030430079 CET	53	53034	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:23.317958117 CET	57762	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:23.345107079 CET	53	57762	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:23.411839008 CET	55435	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:23.447468042 CET	53	55435	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:24.317749977 CET	50713	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:24.344924927 CET	53	50713	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:27.757742882 CET	56132	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:27.784976006 CET	53	56132	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:28.563620090 CET	58987	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:28.590909004 CET	53	58987	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:30.146143913 CET	56579	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:30.173459053 CET	53	56579	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:30.955521107 CET	60633	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:30.982757092 CET	53	60633	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:41.101613045 CET	61292	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:41.128957033 CET	53	61292	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:50.635850906 CET	63619	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:50.674561024 CET	53	63619	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:51.810693026 CET	64938	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:51.838023901 CET	53	64938	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:52.515333891 CET	61946	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:52.542614937 CET	53	61946	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:52.825397968 CET	64938	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:52.852602959 CET	53	64938	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:53.513309956 CET	61946	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:53.540676117 CET	53	61946	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 21:00:53.843341112 CET	64938	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:53.870443106 CET	53	64938	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:54.513367891 CET	61946	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:54.548965931 CET	53	61946	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:55.841628075 CET	64938	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:55.869064093 CET	53	64938	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:56.513411999 CET	61946	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:56.540821075 CET	53	61946	8.8.8.8	192.168.2.3
Nov 27, 2020 21:00:59.883923054 CET	64938	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:00:59.911258936 CET	53	64938	8.8.8.8	192.168.2.3
Nov 27, 2020 21:01:00.528983116 CET	61946	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:01:00.556488991 CET	53	61946	8.8.8.8	192.168.2.3
Nov 27, 2020 21:01:07.425431013 CET	64910	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:01:07.461298943 CET	53	64910	8.8.8.8	192.168.2.3
Nov 27, 2020 21:01:17.016642094 CET	52123	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:01:17.044147015 CET	53	52123	8.8.8.8	192.168.2.3
Nov 27, 2020 21:01:20.918207884 CET	56130	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:01:20.955321074 CET	53	56130	8.8.8.8	192.168.2.3
Nov 27, 2020 21:01:52.775394917 CET	56338	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:01:52.802730083 CET	53	56338	8.8.8.8	192.168.2.3
Nov 27, 2020 21:02:01.549922943 CET	59420	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:02:01.601723909 CET	53	59420	8.8.8.8	192.168.2.3
Nov 27, 2020 21:02:02.646336079 CET	58784	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:02:02.683772087 CET	53	58784	8.8.8.8	192.168.2.3
Nov 27, 2020 21:02:43.095491886 CET	63978	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:02:43.122754097 CET	53	63978	8.8.8.8	192.168.2.3
Nov 27, 2020 21:02:43.675190926 CET	62938	53	192.168.2.3	8.8.8.8
Nov 27, 2020 21:02:43.726286888 CET	53	62938	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 21:00:22.889955044 CET	192.168.2.3	8.8.8.8	0x7c92	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Nov 27, 2020 21:00:22.910965919 CET	192.168.2.3	8.8.8.8	0x465c	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Nov 27, 2020 21:00:22.967278957 CET	192.168.2.3	8.8.8.8	0x9556	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Nov 27, 2020 21:00:22.972989082 CET	192.168.2.3	8.8.8.8	0x8574	Standard query (0)	app.forexliteoptions.com	A (IP address)	IN (0x0001)
Nov 27, 2020 21:00:23.003499985 CET	192.168.2.3	8.8.8.8	0xafb2	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Nov 27, 2020 21:00:23.317958117 CET	192.168.2.3	8.8.8.8	0x3b12	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 21:00:22.916913986 CET	8.8.8.8	192.168.2.3	0x7c92	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 21:00:22.938219070 CET	8.8.8.8	192.168.2.3	0x465c	No error (0)	maxcdn.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 21:00:22.994182110 CET	8.8.8.8	192.168.2.3	0x9556	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 21:00:23.019804001 CET	8.8.8.8	192.168.2.3	0x8574	No error (0)	app.forexliteoptions.com		198.54.115.249	A (IP address)	IN (0x0001)
Nov 27, 2020 21:00:23.030430079 CET	8.8.8.8	192.168.2.3	0xafb2	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Nov 27, 2020 21:00:23.030430079 CET	8.8.8.8	192.168.2.3	0xafb2	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Nov 27, 2020 21:00:23.345107079 CET	8.8.8.8	192.168.2.3	0x3b12	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	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
Nov 27, 2020 21:00:23.107230902 CET	104.16.18.94	443	192.168.2.3	49727	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 27, 2020 21:00:23.108863115 CET	104.16.18.94	443	192.168.2.3	49728	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 27, 2020 21:00:23.112839937 CET	104.16.18.94	443	192.168.2.3	49729	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 27, 2020 21:00:23.366367102 CET	198.54.115.249	443	192.168.2.3	49725	CN=app.forexliteoptions.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Jan 31 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun Jan 31 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 27, 2020 21:00:23.371263981 CET	198.54.115.249	443	192.168.2.3	49726	CN=app.forexliteoptions.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Jan 31 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun Jan 31 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: iexplore.exe PID: 1488 Parent PID: 792

General

Start time:	21:00:20
Start date:	27/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7158b0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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: 2296 Parent PID: 1488

General

Start time:	21:00:21
Start date:	27/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1488 CREDAT:17410 /prefetch:2
Imagebase:	0x1330000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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

Disassembly