ID: 345110
Sample Name: #B30COPY.htm
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 17:56:53
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

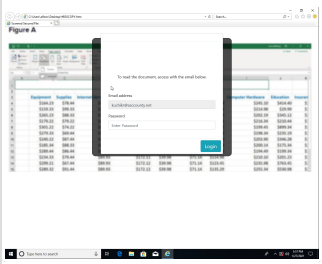
Analysis Report #B30COPY.htm

Overview

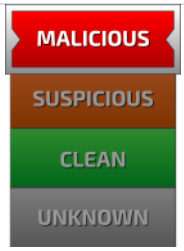
General Information

Sample Name:	#B30COPY.htm
Analysis ID:	345110
MD5:	9fd038de27b73fe..
SHA1:	5100037eb30ce2..
SHA256:	3876920798eb09..

Most interesting Screenshot:



Detection



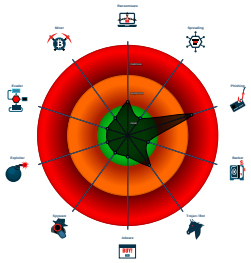
HTMLPhisher

Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- 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: 2076 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4668 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2076 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

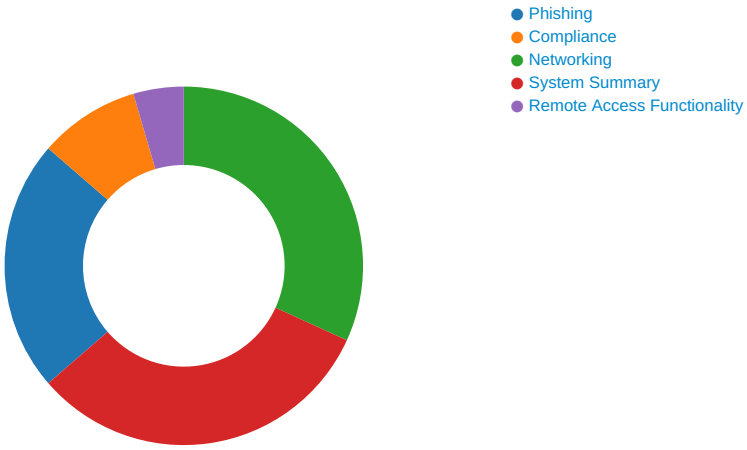
Initial Sample

Source	Rule	Description	Author	Strings
#B30COPY.htm	JoeSecurity_HtmlPhish_7	Yara detected HtmlPhish_7	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Phishing:

Yara detected HtmlPhish_7

Compliance:

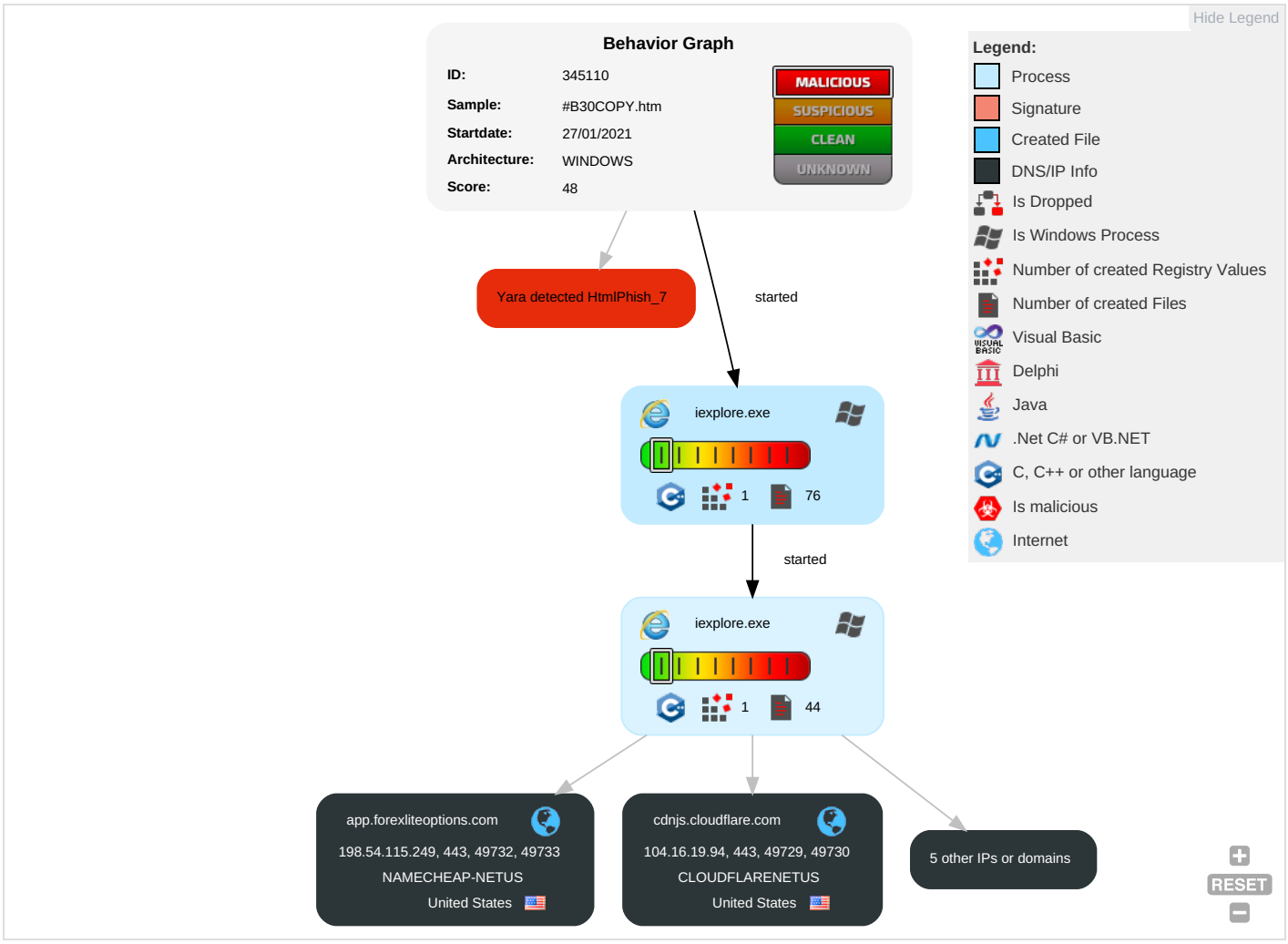
Uses new MSVCR Dlls

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

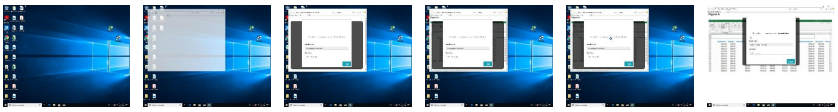
Behavior Graph

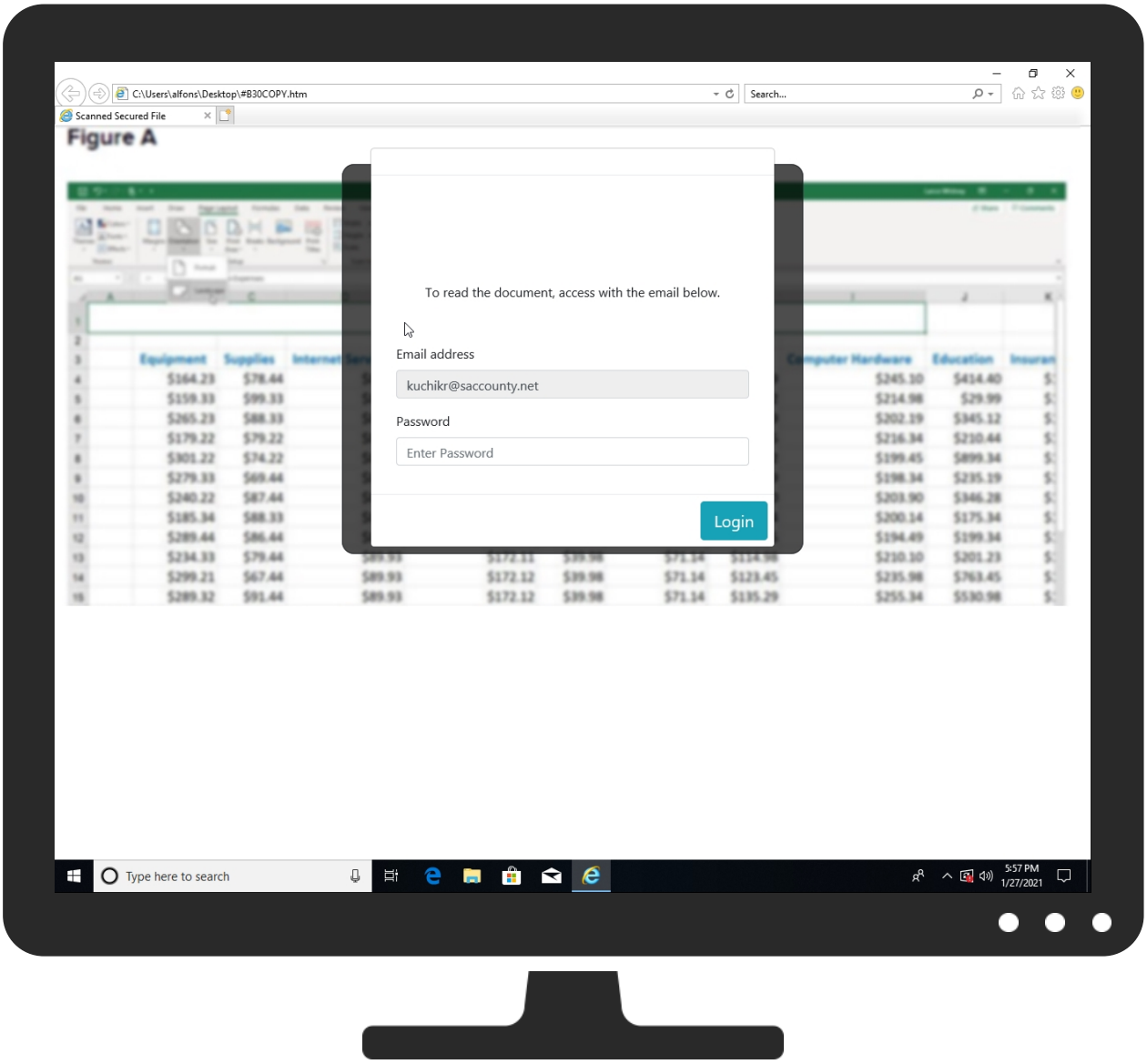


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
app.forexliteoptions.com	4%	Virustotal		Browse
www.stratexe.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
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	

Source	Detection	Scanner	Label	Link
http://https://getbootstrap.com)	0%	Avira URL Cloud	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	
http://https://stratexe.net/coc/realm/send.php	0%	Avira URL Cloud	safe	
http://https://www.stratexe.net/co/Untitled1.jpg	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdnjs.cloudflare.com	104.16.19.94	true	false		high
app.forexliteoptions.com	198.54.115.249	true	false	• 4%, Virustotal, Browse	unknown
www.stratexe.net	154.0.175.244	true	false	• 0%, 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

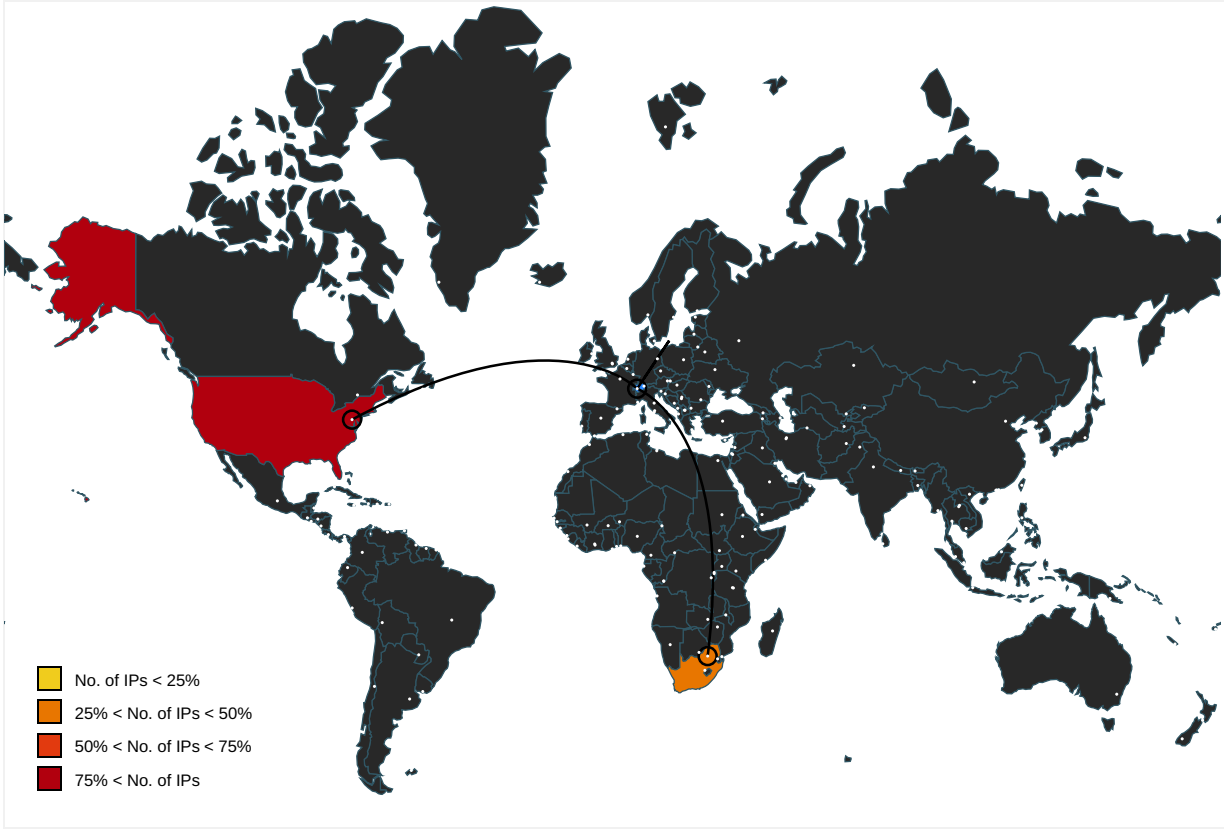
Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/%23B30COPY.htm	true		low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
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	#B30COPY.htm	false		high
http://https://outlook.office.com/mail/inbox	#B30COPY.htm	false		high
http://https://code.jquery.com/jquery-3.1.1.min.js	#B30COPY.htm	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/crypto-js/4.0.0/core.min.js	#B30COPY.htm	false		high
http://www.amazon.com/	msapplication.xml.1.dr	false		high
http://https://solutionsaec-my.sharepoint.com/:x:/g/personal/jblanquart_solutions-aec_com/Eco5JmDEVEFLtBrJ2	#B30COPY.htm	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	#B30COPY.htm	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css	#B30COPY.htm	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://kit.fontawesome.com	585b051251[1].js.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	#B30COPY.htm	false		high
http://https://app.forexliteoptions.com/core/database/xero/css/hover.css	#B30COPY.htm	false	• Avira URL Cloud: safe	unknown
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://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=$	#B30COPY.htm	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://stratexe.net/coc/realm/send.php	#B30COPY.htm	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
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	#B30COPY.htm	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js	#B30COPY.htm	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/crypto-js/3.1.9-1/md5.js	#B30COPY.htm	false		high
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://https://www.stratexe.net/co/Untitled1.jpg	#B30COPY.htm	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.115.249	unknown	United States		22612	NAMECHEAP-NETUS	false
104.16.19.94	unknown	United States		13335	CLOUDFLARENETUS	false
154.0.175.244	unknown	South Africa		37611	AfrihostZA	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345110
Start date:	27.01.2021
Start time:	17:56:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	#B30COPY.htm
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:	20
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:	mal48.phis.winHTM@3/28@7/3
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .htm
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.108.39.131, 209.197.3.24, 172.217.22.202, 209.197.3.15, 104.18.23.52, 104.18.22.52, 172.217.23.74, 172.64.202.28, 172.64.203.28, 23.210.248.85, 51.132.208.181, 152.199.19.161, 95.101.22.125, 95.101.22.134, 51.103.5.159, 20.54.26.129, 51.11.168.160 • Excluded domains from analysis (whitelisted): cds.s5x3j6q5.hwcdn.net, arc.msn.com.nsatc.net, ka-f.fontawesome.com.cdn.cloudflare.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, emea1.notify.windows.com.akadns.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, kit.fontawesome.com.cdn.cloudflare.net, fonts.googleapis.com, client.wns.windows.com, fs.microsoft.com, ajax.googleapis.com, ie9comview.vo.msecnd.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cds.j3z9t3p6.hwcdn.net, par02p.wns.notify.trafficmanager.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	#20030300COPY.htm	Get hash	malicious	Browse	
	#20030300COPY.htm	Get hash	malicious	Browse	
	#20030300COPY.htm	Get hash	malicious	Browse	
	01#Copy.htm	Get hash	malicious	Browse	
	#Ud83d#Udcdevmshares_msgs.htm	Get hash	malicious	Browse	
	Statement.htm	Get hash	malicious	Browse	
	Final_Reports_2020.htm	Get hash	malicious	Browse	
	Final_Report.html	Get hash	malicious	Browse	
	Final_report_2020.html	Get hash	malicious	Browse	
	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-8934 251.html	Get hash	malicious	Browse	
	#U260e#Ufe0fvmsahres__43029812(89201---mssgss-8934 251.htm	Get hash	malicious	Browse	
	Fsc836mx11067098.htm	Get hash	malicious	Browse	
	scan396fx06384866.htm	Get hash	malicious	Browse	
	scan256fx47891482.htm	Get hash	malicious	Browse	
104.16.19.94	http://https://bit.ly/3hDDoTm	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://ninjutsu.4ryu.com/.well-known/pki-validation/zombaiogw_1_1/print_recipe.php?living=ytpr1h11zw0qw0&south=difference&slide=during	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://surl.me/vy4l	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://u15974653.ct.sendgrid.net/ls/click?upn=sKo8P2XHLOhqpgLcALrpHsAMymMPQ9pJ-2BnCP9l5luXmX2tau-2FkmeQME9D69RU7ffQBYwWBrDSW94kS5u6ig5BmkhgBhgQJfm-2BsLwvjPlmdPdsXD4ILOaqVNEwgY7GAZQPkafmgyIOS5FU-2B6124ooi1O-2FMB47qUlmVhTTnK6qV5fGlsBAy7itOSHfP1wikhvsiyeK_Y89n8cg5DiKkjVvtw-2FYSjk3JbqBqCNqd4QE5c0z9p4IJ6aN66chjxOUHcribC2kbrQ6ua83fMfn3Hnb3TofbErA9L2X-2BpZpbvzOnYxCl6WSRvjbd6cnTXhRnH1-2Btzg-2FEpNckJ170lMbhRvVxgpvwWV6rRyYLwNDxpt3Im1lgyNi-2B-2B86Pp03BP8O3y-2Bw2BSUYNj8fK3irR9dYwZuWCkvZJ3fJURjdr0uD0itVZut-2BhVs-3D	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/font-awesome/4.1.0/fonts/fontawesome-webfont.eot?
	http://https://j.mp/38NwiZZ	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://lokalny-biznes.eu/modules/mod_simplefileuploadv1.3/elements/reactivation/indextest.php?youll=enwht11p10sc0&picture=call&please=gave	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://pinpoint-insights.com/interx/tracker?op=click&id=107b4.3e3b&url=https%3A%2F%2Fpinpoint-insights.com%2Finterx%2Funsubscribe%3Fid%3D107b4.3e3b%26type%3Dnormal&_hC=D7C07475	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/flickity/1.0.0/flickity.min.css
	http://https://pinpoint-insights.com/interx/tracker?op=click&id=107b4.3e3b&url=https%3A%2F%2Fpinpoint-insights.com%2Finterx%2Funsubscribe%3Fid%3D107b4.3e3b%26type%3Dnormal&_hC=D7C07475	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/flickity/1.0.0/flickity.min.css

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
154.0.175.244	#20030300COPY.htm	Get hash	malicious	Browse	
	#20030300COPY.htm	Get hash	malicious	Browse	
	#20030300COPY.htm	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.stratexe.net	#20030300COPY.htm	Get hash	malicious	Browse	• 154.0.175.244
	#20030300COPY.htm	Get hash	malicious	Browse	• 154.0.175.244
	#20030300COPY.htm	Get hash	malicious	Browse	• 154.0.175.244
app.forexliteoptions.com	#20030300COPY.htm	Get hash	malicious	Browse	• 198.54.115.249
	#20030300COPY.htm	Get hash	malicious	Browse	• 198.54.115.249
	#20030300COPY.htm	Get hash	malicious	Browse	• 198.54.115.249
	01#Copy.htm	Get hash	malicious	Browse	• 198.54.115.249
	#Ud83d#Udcdevmshares_msgs.htm	Get hash	malicious	Browse	• 198.54.115.249
	Statement.htm	Get hash	malicious	Browse	• 198.54.115.249
	Final_Reports_2020.htm	Get hash	malicious	Browse	• 198.54.115.249
	Final_Report.html	Get hash	malicious	Browse	• 198.54.115.249
	Final_report_2020.html	Get hash	malicious	Browse	• 198.54.115.249
	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
	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
cdnjs.cloudflare.com	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	The Mental Health Center.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	Monday, January 25, 2021 222135-ATT+72308645308805 6636775.htm	Get hash	malicious	Browse	• 104.16.18.94
	PAYMENT INFO.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	PAYMENT INFO.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	1_25_2021 11_20_30 a.m., [Payment 457 CMSupportDev].html	Get hash	malicious	Browse	• 104.16.19.94
	Payment_[Ref 72630 - joe.blow].html	Get hash	malicious	Browse	• 104.16.19.94
	INVOICES & STATEMENTS_02201.htm	Get hash	malicious	Browse	• 104.16.19.94
	#U03bd#U03bf#U0456#U0441#U0435m#U0430#U0456l202154095982f#U0433#U03bfm+19792193827 19792193827.HTM	Get hash	malicious	Browse	• 104.16.18.94
	T&S INVC#019.html	Get hash	malicious	Browse	• 104.16.19.94
	4892.htm	Get hash	malicious	Browse	• 104.16.19.94
	4892.htm	Get hash	malicious	Browse	• 104.16.19.94
	20202237F.html	Get hash	malicious	Browse	• 104.16.18.94
	Release Pending messages on account.html	Get hash	malicious	Browse	• 104.16.19.94
	Payment Advice.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	Payment Advice.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	ESPP.docx	Get hash	malicious	Browse	• 104.16.19.94
	ESPP.docx	Get hash	malicious	Browse	• 104.16.18.94
	Voicemail wav.html	Get hash	malicious	Browse	• 104.16.18.94

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	AE-808_RAJEN.exe	Get hash	malicious	Browse	• 68.65.122.156
	RFQ Tengco_270121.doc	Get hash	malicious	Browse	• 198.54.122.60

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	quote20210126.exe.exe	Get hash	malicious	Browse	• 198.54.117.215
	MV TAN BINH 135.pdf.exe	Get hash	malicious	Browse	• 198.54.116.236
	IMG_155710.doc	Get hash	malicious	Browse	• 199.192.18.134
	bXFjrxjRlb.exe	Get hash	malicious	Browse	• 198.54.117.215
	Dridex-06-bc1b.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	Dridex-06-bc1b.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	winlog(1).exe	Get hash	malicious	Browse	• 198.54.117.216
	Revise Bank Details_pdf.exe	Get hash	malicious	Browse	• 198.54.116.236
	SecuriteInfo.com.BehavesLike.Win32.Generic.tz.exe	Get hash	malicious	Browse	• 198.187.31.7
	SecuriteInfo.com.Trojan.DownLoader36.37393.29158.exe	Get hash	malicious	Browse	• 198.187.31.7
	Payment Swift Copy_USD 206,832,000.00.pdf.exe	Get hash	malicious	Browse	• 198.54.116.236
	INGNhYonmgtGZ9Updf.exe	Get hash	malicious	Browse	• 198.54.117.244
	DSksliT85D.exe	Get hash	malicious	Browse	• 199.188.200.97
	file.exe	Get hash	malicious	Browse	• 198.54.116.236
	Tebling_Resortsac_FILE-HP38XM.htm	Get hash	malicious	Browse	• 104.219.248.112
	file.exe	Get hash	malicious	Browse	• 198.54.116.236
	RevisedPO.24488_pdf.exe	Get hash	malicious	Browse	• 198.54.117.215
	74725794.exe	Get hash	malicious	Browse	• 198.54.122.60
CLOUDFLARENETUS	98.doc	Get hash	malicious	Browse	• 172.67.156.114
	DHL-INVOICE RECEIPT.html	Get hash	malicious	Browse	• 172.67.133.221
	Luminar4 (4.4).exe	Get hash	malicious	Browse	• 104.21.85.23
	SecuriteInfo.com.BehavesLike.Win32.PUPXAA.gc.exe	Get hash	malicious	Browse	• 172.67.169.213
	IMG-47901.exe	Get hash	malicious	Browse	• 104.21.19.200
	SecuriteInfo.com.BehavesLike.Win32.PUPXAA.gc.exe	Get hash	malicious	Browse	• 172.67.169.213
	SecuriteInfo.com.BehavesLike.Win32.SoftPulse.gc.exe	Get hash	malicious	Browse	• 172.67.169.213
	Purchase Order.xlsx	Get hash	malicious	Browse	• 104.21.47.75
	SecuriteInfo.com.BehavesLike.Win32.PUPXAA.gc.exe	Get hash	malicious	Browse	• 172.67.169.213
	SecuriteInfo.com.BehavesLike.Win32.SoftPulse.gc.exe	Get hash	malicious	Browse	• 172.67.169.213
	SecuriteInfo.com.BehavesLike.Win32.SoftPulse.gc.exe	Get hash	malicious	Browse	• 104.21.27.240
	SecuriteInfo.com.Generic.mg.d82abc4e3bc3179d.exe	Get hash	malicious	Browse	• 172.67.169.213
	SecuriteInfo.com.BehavesLike.Win32.SoftPulse.gc.exe	Get hash	malicious	Browse	• 104.21.27.240
	SecuriteInfo.com.BehavesLike.Win32.PUPXAA.gc.exe	Get hash	malicious	Browse	• 172.67.169.213
	SecuriteInfo.com.Heur.30497.xls	Get hash	malicious	Browse	• 172.67.198.109
	SecuriteInfo.com.Exploit.Siggen3.8790.14645.xls	Get hash	malicious	Browse	• 172.67.200.147
	SecuriteInfo.com.Trojan.DOC.Agent.ATB.11104.xls	Get hash	malicious	Browse	• 172.67.201.174
	SecuriteInfo.com.Trojan.Inject4.6746.26345.exe	Get hash	malicious	Browse	• 162.159.130.233
	SecuriteInfo.com.Trojan.Inject4.6746.26345.exe	Get hash	malicious	Browse	• 162.159.134.233
	case (2553).xls	Get hash	malicious	Browse	• 104.21.44.135
AfrihostZA	bin.sh	Get hash	malicious	Browse	• 169.173.126.123
	New order.exe	Get hash	malicious	Browse	• 154.0.163.40
	Review bank details.exe	Get hash	malicious	Browse	• 154.0.167.156
	3-321-68661.xls	Get hash	malicious	Browse	• 197.242.151.164
	#20030300COPY.htm	Get hash	malicious	Browse	• 154.0.175.244
	http://https://motswedingms.co.za/wp-content/axis/oauth/site/service/demp.php?email=kazou.mvl@cm.be	Get hash	malicious	Browse	• 154.0.173.185
	#20030300COPY.htm	Get hash	malicious	Browse	• 154.0.175.244
	DOCX9-29827.doc	Get hash	malicious	Browse	• 154.0.165.27
	#20030300COPY.htm	Get hash	malicious	Browse	• 154.0.175.244
	xJbFpiVs1l	Get hash	malicious	Browse	• 169.85.190.120
	bdOPjE89ck.dll	Get hash	malicious	Browse	• 169.217.238.137
	document-180101256.xls	Get hash	malicious	Browse	• 154.0.174.32
	document-180101256.xls	Get hash	malicious	Browse	• 154.0.174.32
	document-1775113270.xls	Get hash	malicious	Browse	• 154.0.174.32
	document-1775113270.xls	Get hash	malicious	Browse	• 154.0.174.32
	document-1846403542.xls	Get hash	malicious	Browse	• 154.0.174.32
	document-1876740618.xls	Get hash	malicious	Browse	• 154.0.174.32
	document-1846403542.xls	Get hash	malicious	Browse	• 154.0.174.32
	document-1876740618.xls	Get hash	malicious	Browse	• 154.0.174.32
	document-1859917192.xls	Get hash	malicious	Browse	• 154.0.174.32

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	33ffr.dll	Get hash	malicious	Browse	• 198.54.115.249 • 104.16.19.94 • 154.0.175.244
	SecuriteInfo.com.ArtemisCAA9F750565C.dll	Get hash	malicious	Browse	• 198.54.115.249 • 104.16.19.94 • 154.0.175.244
	smf53wmr.zip.dll	Get hash	malicious	Browse	• 198.54.115.249 • 104.16.19.94 • 154.0.175.244
	xziu6ib2.zip.dll	Get hash	malicious	Browse	• 198.54.115.249 • 104.16.19.94 • 154.0.175.244
	cfsuggg.rar.dll	Get hash	malicious	Browse	• 198.54.115.249 • 104.16.19.94 • 154.0.175.244
	ci0v2ix.rar.dll	Get hash	malicious	Browse	• 198.54.115.249 • 104.16.19.94 • 154.0.175.244
	ioqjfxnm.dll	Get hash	malicious	Browse	• 198.54.115.249 • 104.16.19.94 • 154.0.175.244
	ij80czph.dll	Get hash	malicious	Browse	• 198.54.115.249 • 104.16.19.94 • 154.0.175.244
	Rolled Alloys Possible Infection.docx	Get hash	malicious	Browse	• 198.54.115.249 • 104.16.19.94 • 154.0.175.244
	ntd7zy47.dll	Get hash	malicious	Browse	• 198.54.115.249 • 104.16.19.94 • 154.0.175.244
	Quotation.exe	Get hash	malicious	Browse	• 198.54.115.249 • 104.16.19.94 • 154.0.175.244
	r4bf43.dll	Get hash	malicious	Browse	• 198.54.115.249 • 104.16.19.94 • 154.0.175.244
	ktyedjx6x.dll	Get hash	malicious	Browse	• 198.54.115.249 • 104.16.19.94 • 154.0.175.244
	xfagxh61l.dll	Get hash	malicious	Browse	• 198.54.115.249 • 104.16.19.94 • 154.0.175.244
	ep9n62vf.dll	Get hash	malicious	Browse	• 198.54.115.249 • 104.16.19.94 • 154.0.175.244
	SecuriteInfo.com.Generic.mg.0f80eecd45dc9b78.dll	Get hash	malicious	Browse	• 198.54.115.249 • 104.16.19.94 • 154.0.175.244
	SecuriteInfo.com.Generic.mg.aeca39dc4ac4ba79.dll	Get hash	malicious	Browse	• 198.54.115.249 • 104.16.19.94 • 154.0.175.244
	SecuriteInfo.com.Generic.mg.faa94a7eb8be850d.dll	Get hash	malicious	Browse	• 198.54.115.249 • 104.16.19.94 • 154.0.175.244
	SecuriteInfo.com.Generic.mg.cd76e3dec70533d8.dll	Get hash	malicious	Browse	• 198.54.115.249 • 104.16.19.94 • 154.0.175.244
	SecuriteInfo.com.Generic.mg.7e70f13d976bdf3a.dll	Get hash	malicious	Browse	• 198.54.115.249 • 104.16.19.94 • 154.0.175.244

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{34802B54-610C-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{34802B54-610C-11EB-90E5-ECF4BB570DC9}.dat	
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8504149491458906
Encrypted:	false
SSDEEP:	96:rnZEZO219Wntcbf2EDKMVkLqGRQuxfeEi6X:rnZEZO219Wnt8f2xMx9wfeMX
MD5:	CD7E98AFD290EA2DE1DD4C3DFB771656
SHA1:	82ECA934B281BF3B088FAD6649E2C6D1077C0B5F
SHA-256:	ACDE441CEEE2B2D9B4E1F49C1017DF4F129550195964B69DB7862BA04636DD8C
SHA-512:	C83EBCE811CD5660A241182AC67A42AD5E2DA1818434043EAED75003F210D2C4EF41D23CCF3CC92F1B8540C76DE34764A2A7F9B140C22B4BD20BFC682D745D 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\{34802B56-610C-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28256
Entropy (8bit):	1.9217719619519569
Encrypted:	false
SSDEEP:	96:rXZOQu6gBSNFjh2ckWCMxYTDYWXASC7cNr:rXZOQu6gkNFjh2ckWCMxYTDYWw4Nr
MD5:	568BE5FDFCFA731003C8584373074717
SHA1:	5FD35F972A704EF3AB0C067604A14A52F02455C9
SHA-256:	72BFB4DC4A723E2EB1F6E6DC19B008C7BFA57653F9C1664ACCF0BEAECDAAF158
SHA-512:	E7F413041799F10E12B17A66A167FEA3732F3C3A2D9CF4DFD6358CAE1280DE3C127DEEA37A7A2A616974A4BA8532D08FC9D73E8E99F6D4D715508B1D1E03C43 8
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\{34802B57-610C-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5672083701096227
Encrypted:	false
SSDEEP:	48:IwSGcprzGwpaaG4pQOGrapbSFrGQpK/G7HpResTGIpG:rmZtQa6ABSFFAOTe4A
MD5:	64B260BFE6F938DB7B6A3906166BC058
SHA1:	DBA52ED505CB8B6A21341D4277D7F9985011506C
SHA-256:	CC320B61976B78E9D85BCA0820D8242EBED0EE7A56FA204924348DA0FB580519
SHA-512:	3D0A9CE07CE9B545333DF17F05B63BE7EFFB31C9E9428C28AB4ACB2C40E196CD023D2E8F4DC84C0FEF4959FAED5B03FDCFB12497FE08D05DCC449454FB9BF D20
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):	657
Entropy (8bit):	5.101120555442407
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEV34CnWimI002EtM3MHdNMNxOEV34CnWimI00ONVbkEtMb:2d6NxOwSZHKd6NxOwSZ7Qb

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
MD5:	FC81AC46BF2B90E8FCD8D19EA0EC4795
SHA1:	8FE609CB003DDF6902794415447AEB968D805DA7
SHA-256:	FA00D38E87631DDD79210CFFDA1AD0A24562FE30679847D204F8BBAED940ABCA
SHA-512:	12D11CC0CB836234597A74CCD971D433CA7281C1CB3DCA06BB945E0655DEEC5547F876EB7E1F54A17242C9FAD9D95AF00D28224D1DAE08DCA32516D07A497C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x0ab83d43,0x01d6f519</date><accdate>0x0ab83d43,0x01d6f519</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>0x0ab83d43,0x01d6f519</date><accdate>0x0ab83d43,0x01d6f519</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):	654
Entropy (8bit):	5.118587048957074
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2k4WTxnWimI002EtM3MHdNMNxe2k4WTxnWimI00ONkak6EtMb:2d6NxrUSZHKd6NxrUSZ72a7b
MD5:	F701070076D0ED2F7C446559AEC24D80
SHA1:	1609CFFEAD5D79D39018D2D32240E9B16C07D682
SHA-256:	1608253BDA63F565380700D6AB161BD1114FF3872AC113D415BACC6A090FEA04
SHA-512:	7AE97F9DF69A7B58C9EEF7750F447EAA0B8AEA77EB022D88FEE561138ED43074327C7BC9244E372D5CA35EE9040C166D7CBF5541AB78975248DCFCAC3E94E3C4
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x0ab11622,0x01d6f519</date><accdate>0x0ab11622,0x01d6f519</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>0x0ab11622,0x01d6f519</date><accdate>0x0ab11622,0x01d6f519</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):	663
Entropy (8bit):	5.118928188816968
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLV34CnWimI002EtM3MHdNMNxvLV34CnWimI00ONmZEtMb:2d6NxvNSZHKd6NxvNSZ7Ub
MD5:	99124375B3D4AB5BF6212FDACF821C20
SHA1:	5834CB443A353BF07B6CADF451865840258415D3
SHA-256:	99BF9D4721C286B35CC4ED66FA6FD8BCDB1CAA0B54C7B5D754552394C9BC0C73
SHA-512:	4F58A07BC6D0061EB3E6B35F632B1C30D0AB77BC976C8E686BDEBE485548BC9C79F9F226F6DDBC9664914D301DBC66E3D867CDA3C49D82BB0DEB9B2E1CE2DC4
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x0ab83d43,0x01d6f519</date><accdate>0x0ab83d43,0x01d6f519</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>0x0ab83d43,0x01d6f519</date><accdate>0x0ab83d43,0x01d6f519</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):	648
Entropy (8bit):	5.063057130035918
Encrypted:	false
SSDEEP:	12:TMHdNMNxi6hxonWimI002EtM3MHdNMNxi6hxonWimI00ONd5EtMb:2d6NxkSZHKd6NxkSZ7njb
MD5:	2E1E04EEAC5E21EF483D60FFA54F80DD
SHA1:	88DF16640F5C2F5E95349195663691DD21BA26F7
SHA-256:	8CC2C288E7DA46AE15EAB07DE1A82BE102F73403216BFE98DEF4220147619026

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
SHA-512:	2B0A1C165B2835F76988FF815CC5187E170C322406A80D5DAA9210C0B185CACAC9F3F41FBB8DA79AD90CBD15CA676F9E417327D785915BA7B0019BDAD641CD D
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x0ab5dada,0x01d6f519</date><acc date>0x0ab5dada,0x01d6f519</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>0x0ab5dada,0x01d6f519</date><accdate>0x0ab5d ada,0x01d6f519</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):	657
Entropy (8bit):	5.131713386378705
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwV34CnWimI002EtM3MHdNMNxhGwV34CnWimI00ON8K075EtMb:2d6NxQUSZHKd6NxQUSZ7uKajb
MD5:	01954EA3F90107C6A698C6A5D2CE429C
SHA1:	C32886EC986634EE4CB7129A686F34AEF60C7F48
SHA-256:	5896E798E87810B4C303C64D831E82CB61EBAB8A9EE1BD14F60B5242ACD631BD
SHA-512:	D1D8D9F828E97B29FD5B6F68E1E9F1AE853F700E40BF4BB96969A1A6B46B3A6F8FD2D6D40B42B403F376FFC1BB31220211E83DCF670E16D32BA3C588FE39557
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x0ab83d43,0x01d6f519</date>< accdate>0x0ab83d43,0x01d6f519</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>0x0ab83d43,0x01d6f519</date><accdate>0 x0ab83d43,0x01d6f519</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):	654
Entropy (8bit):	5.0473803447202386
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n6hxonWimI002EtM3MHdNMNx0n6hxonWimI00ONxEtMb:2d6Nx0jSZHKd6Nx0jSZ7Vb
MD5:	65B0F07C88791BC04C31AD4D2EA81831
SHA1:	D12A5DA5C8D3969501751388D8250C048C4E0DBB
SHA-256:	717BA9F9A1CF4B8846A3DEF6AE97E3E98287E1DC6E2A0C140C57AAA766238071
SHA-512:	B6956EA7F8E74A4B5ED42B66EE051E95D1298AB885A4F4BA0179A38DB9881E215D03A0A729E7A91BB7E314F00C3159B52E3F53E8979497C28F72DC56DF5197F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x0ab5dada,0x01d6f519</date><a ccdate>0x0ab5dada,0x01d6f519</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>0x0ab5dada,0x01d6f519</date><accdate>0x0 ab5dada,0x01d6f519</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):	657
Entropy (8bit):	5.0880963045597545
Encrypted:	false
SSDEEP:	12:TMHdNMNxx6hxonWimI002EtM3MHdNMNxx6hxonWimI00ON6Kq5EtMb:2d6NxVSZHKd6NxVSZ7ub
MD5:	4BCB6716A392FDB4B6C438773B1CBF4F
SHA1:	F827E5F80833A58E1510A5ACFADBA0C54550B7A7
SHA-256:	9DECB68FDF2F39325C5E31D0A59F938CA929FD3257DB3F588BC1BFEE19A5D6EF
SHA-512:	BC5106FD4C6C33D0B05E8C9ED990016E8F55D98FB45D4F8FF2B803ACB192BB83C8FC363B0A9D64017048EF708892B9D9514207AC657B04DDC3C38BF9A8FCAC 2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x0ab5dada,0x01d6f519</date><accdate>0x0ab5dada,0x01d6f519</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>0x0ab5dada,0x01d6f519</date><accdate>0x0ab5dada,0x01d6f519</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):	660
Entropy (8bit):	5.129402549435897
Encrypted:	false
SSDEEP:	12:TMHdNMNxcEQ5fnWimI002EtM3MHdNMNxcEQ5fnWimI00ONVEtMb:2d6NxUSZHKd6NxUSZ71b
MD5:	FC85B9C8433EB1B49B0DE798A572816A
SHA1:	9014E0FFE0BD5D8F181AA974C8D65D2B7AE1BE7A
SHA-256:	9A331A01EBD6F57F9D454826DC55BA170FAAAF30E1C76512A91D318D9F8ECAFF
SHA-512:	677A5BDACF541D7D0D7DA8DF996FAF875256D3F7C14552859E2B5E5F8FD38D959F1549EDA57948F60DDB33E6FF372AC662BCF06C29A087F077DFC55EABC306B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x0ab37882,0x01d6f519</date><accdate>0x0ab37882,0x01d6f519</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>0x0ab37882,0x01d6f519</date><accdate>0x0ab37882,0x01d6f519</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):	654
Entropy (8bit):	5.115073478584019
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnEQ5fnWimI002EtM3MHdNMNxfnEQ5fnWimI00ONe5EtMb:2d6Nx5SZHKd6Nx5SZ7Ejb
MD5:	137F9A1D4036215EE9E88143B3F196D5
SHA1:	68502E731125FCA513A537FE64062C2214633537
SHA-256:	B1F6A992268C3F2223995FBCEB151818F209E8D889916A5C6559C32E2F9C3453
SHA-512:	C4E284AD98A47CAFCB7F1DD89767851613A67CDBB0DFA704BF43EFCA769F1608D97E8E0A7304DCA7F6B765B75B4C6D884D6698E97645C57FF5DBAFACF7E0F71
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x0ab37882,0x01d6f519</date><accdate>0x0ab37882,0x01d6f519</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>0x0ab37882,0x01d6f519</date><accdate>0x0ab37882,0x01d6f519</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\4PB7FJMT\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
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\bootstrap.min[1].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}h tml{font-family:sans

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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
Reputation:	high, very likely benign file
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"),requir e("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.pro totype.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\4PB7FJMT\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:	53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D69067E 65
Malicious:	false
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.do cument?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.c all(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,t oArray: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\4PB7FJMT\jquery-3.2.1.slim.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
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:	CAB8C4AFA1D8E3A8B7856EE29AE92566D44CEEAD70C8D533F2C98A976D77D0E1D314719B5C6A473789D8C6B21EBB4B89A6B0EC2E1C9C618FB1437EBC77D3A 269
Malicious:	false
IE Cache URL:	http://https://code.jquery.com/jquery-3.2.1.slim.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\jquery-3.2.1.slim.min[1].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\B87Z87FM\585b051251[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	10866
Entropy (8bit):	5.182477446178365
Encrypted:	false
SSDEEP:	192:BBHN42S+9SZRvACpilthFzoXnemF+shSGnZ+PPxQDqv7jh81Q5l8OcchIlzbCn:HRCfhFzevnEZ/h81Q5l8OsE
MD5:	4B900F0AF3BBDA85E1077C8EC8C83831
SHA1:	7E7015965195F25AFA3A47BE2108278AD6A0A4AC
SHA-256:	7943D6D067DB8587E9FB675F0D2CC78D6C90C91B187CF8642A3F52FF91381685
SHA-512:	2CD82E0DCD1381447522CFFD610136513323E5D2980FAE730801FE8BBA580FF7FDF9CB8D2E9AC794D6F2FB59C724EDA71BECE7CAA72C775BC963E1A54B30EBCB
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","baseUrlKit":"https://kit.fontawesome.com","detectConflictsUntil":null,"iconUploads":{},"id":132286382,"license":"free","method":"css","minify":{"enabled":true},"token":"585b051251","v4FontFaceShim":{"enabled":false},"v4shim":{"enabled":true},"version":"5.15.2"};.!function(t){"function"==typeof define&&define.amd?define("kit-loader",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 r=Object.getOwnPropertySymbols(t);e&&(r=r.filter((function(e){return Object.g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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
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\B87Z87FM\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:	0D40BCCAA59FEDECF7243D63B33C42592541D0330FEFC78EC81A4C6B9689922D5B211011CA4BE23AE22621CCE4C658F52A1552C92D7AC3615241EB640F8514BB
Malicious:	false
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\jquery.min[1].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\B87Z87FM\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\B87Z87FM\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
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\NUEPGTR9\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):	4.82979949483045
Encrypted:	false
SSDEEP:	192:SP6hT1bIl4w0QUmQ10PwKLaAu5CwWavpHo4O6wgLPbJVR8XD7mycP:5hal4w0QK+PwK05eavpmgPPeXD7mycP
MD5:	1848E71668F42835079E5FA2AF6CF4A8
SHA1:	6AE345E2FEB8C2A524E7CF9E22A3A87BAEE60593
SHA-256:	D7CC3C57F9BDA4C6DCB83BB3C19F2F2AA86ECEC6274E243CD4EC315AE8E30101
SHA-512:	24E0AF4EC32A9AAB61D9E1AF9B2083F2D13CC98961B5E32BB613A02FEEF63F5F30C3B21C6308A4A204D981D77C86F09E221D0DB7B051A3538ACE07E727F29F58
Malicious:	false
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.2/css/free-v4-shims.min.css?token=585b051251

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\free-v4-shims.min[1].css	
Preview:	/*!. * Font Awesome Free 5.15.2 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\NUEPGTR9\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):	4.728636851806783
Encrypted:	false
SSDEEP:	768:5Uh31IPiyXNq4YxBowbgJlkwF//zMQyYJYX9Bft6VSz8:5U0PxXE4YXJgndFTfy9lt5Q
MD5:	4ECC071B77D6B1790FA9FB8A5173F972
SHA1:	B44FCBAAC4F3AA7381D71DE20064AC84B0B729D1
SHA-256:	8C7BBA7DEB64FF95E98F7AC8CD0D3B675A4BCF02F302E57EDC5A1D6FA3D6CF94
SHA-512:	7CC1D04078B5917269025B6F37C7DDD83A0A5A0C5840E2A6E99ADFE2FB3E2242C626F25315480ADCD725C855AD2881DDF672B6FC1D793377C2D16FF38EAF69
Malicious:	false
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.2/css/free.min.css?token=585b051251
Preview:	/*!. * Font Awesome Free 5.15.2 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\PEJLKQA8\Untitled1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 799 x 502, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	317768
Entropy (8bit):	**7.991343148175131**
Encrypted:	**true**
SSDEEP:	6144:hR/TlQa55WXUAXG0RCsrYPy/hRhvzCgfNdSzguv+hQo+p7jv:XLlFPWkBcYszvxdPOo+Bjv
MD5:	8070A602EE62C504688EAAFBB6CDD7D8
SHA1:	FE19A5B99A9791F1E450BEC86B1A99A5BE990179
SHA-256:	2E0DB89BE0DB86ED485D0C7505C0EF0FF41D752FB322DEDBAA31FD64DAE4FAE3
SHA-512:	3BEC8909339F3507A4A3B351678D9AE9869D67848AFD9B881F3DC6269647430576287416327771258BA599A661F0FEA72D41C9EE73B0F5D2C52A3FC11E54F89D
Malicious:	false
IE Cache URL:	http://https://www.stratexe.net/co/Untitled1.jpg
Preview:	.PNG.....IHDR.....p1... .IDATx^..{e.u%.n...htb....,.%.=..7o.'....-..EY.....f.....}k.:u..b7)J,P..'T..{..+.....U*..WPA%.*...l.dc.+..*5d.*P..!.....f#T.GV...TPG..F:..*.....yf. .W2.1.:.....@.@u\C...1..1..|:.Z.WP.*.f...?.]._.bT..U.dCT....2>.....6w..."..Y.....o.a,.p.....2.....H_.....?L.....9....5.U.....0....u...;.c8.P....*..:..&..*.b<.R.h..luP.7D..2O.P'....o. .?.2.:.....C>.g....A.P..>t||.... 2""....y~..e$...V.D..?.|.3{^6.h0D....~..1.\G..F..@.V5.a....P.+Q Q Q Q Q Q Q Q Q..M.....G.....(..z...x...-<\].....ps..^_.....[.i,,,bia.....].....K8.|.S3S.." .....,.x.FT...jF../.....>r..:.[~Qhcp./1.A.A._.9.t..#.w..+..w.....OM...K8.a..3.hV.....G.J.H.H.H.H.H.H.H..AS..l.9.J.Q.v%\.....x....{...M....q..=...h.Zh...0=..'.<.....ze..u....'....k8. <.Z.aJ...|._.xD A....._c.H..p*..x^.....+..R...t.c..s....r.#.U.....>.....p.SK.x.....k/...i....h.....Z.|.@.@.@.@.@.@.@.@..1....C.....m../..[w..h...9.NO....]..+Wp.....x...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\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\Temp\~DF92CAE777F9950E09.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4780660114836554
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRK9l8fR69lTqTO71yQWp:c9lLh9lLh9lIn9lIn9loK9lo69lWKG
MD5:	9632FD10F1BE6B3EB793AD218E652F2A
SHA1:	ED9A0439FC12C655E19519C4C23E25CC6ED2DB89
SHA-256:	ACEE258BBAC89F457376BD41A8E35D3EAAA29EA6027CD7580BFA42412C903CD8
SHA-512:	2DB75F46C233894428DB4B154A4A6EC991AB822A8D7779C9CF3F60CF23104BEE423AAE907DEA479226277D2E2AC8CF8CB2F517A5E3953B32347A866A114893E
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFFA05A35BBB43BEE5.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	36017
Entropy (8bit):	0.6047189593228587
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+qMWfTITvxeSQxZEGkxZEniS6SpSk70SC:kBqoxKAuvScS+qMWfMDWXASC
MD5:	5D9AF1D31494BE282EF1FAA9AB7A77F3
SHA1:	D73A1CEE2C53CABAC3F4513CB25C44F14BC585D1
SHA-256:	361FDF14DBF0C79680C0EF002F60E29E58E9E64FC7A168BE1720F72A7EB08A3E
SHA-512:	F8336FB70A041BAC3AE2E84615478DB0C7B6F229578E58D477F7661693C1BAEB9EBAFEAD0AFE3C344D7B6BC2D1F1575EA313D30F98789C91BDFDF99EA0BE5E 21
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFFE549B178B65E1B5.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
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):	4.739209373527315

General

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:	#B30COPY.htm
File size:	17020
MD5:	9fd038de27b73fe352def384cf076995
SHA1:	5100037eb30ce2b98e491196ccf508dfd18414d9
SHA256:	3876920798eb09d4e08654d5eb1c2c1d5760f39a61f3222 0472362b2ba26adce
SHA512:	17e82f662814a2abebf3c160b559bfff197049f0e9a77b8a 3d24aa21c466f533f479985dfd928ba9c672e836a2474b5 372b69d10bcc7daf6fba8e67a0dc5245a
SSDEEP:	192:1/VAbPtzo2B2PThJIhwVIhwVIhwVIhwVrBolXkW4U UqR+5ZDb45:nAb1MhhhoHv2u
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

Total Packets: 86

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 17:57:43.934340954 CET	49729	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:43.935323000 CET	49730	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:43.935765028 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:43.956933022 CET	49732	443	192.168.2.5	198.54.115.249
Jan 27, 2021 17:57:43.956996918 CET	49733	443	192.168.2.5	198.54.115.249
Jan 27, 2021 17:57:43.974334002 CET	443	49729	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:43.974437952 CET	49729	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:43.975084066 CET	49729	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:43.975256920 CET	443	49730	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:43.975383997 CET	49730	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:43.975733995 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:43.975815058 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:43.976310015 CET	49730	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:43.976567030 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.014843941 CET	443	49729	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.016140938 CET	443	49730	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.016622066 CET	443	49731	104.16.19.94	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 17:57:44.016819000 CET	443	49729	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.016836882 CET	443	49729	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.016920090 CET	49729	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.016957998 CET	49729	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.017328024 CET	443	49730	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.017345905 CET	443	49730	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.017421007 CET	49730	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.017457008 CET	49730	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.025629997 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.025662899 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.025727034 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.025752068 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.072238922 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.072666883 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.072845936 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.072923899 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.073002100 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.073466063 CET	49729	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.074127913 CET	49729	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.086221933 CET	49730	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.086576939 CET	49730	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.112169027 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.112607956 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.112637043 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.112663031 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.112708092 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.112755060 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.112795115 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.112823963 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.112848997 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.113236904 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.113317013 CET	443	49729	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.113976002 CET	443	49729	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.115752935 CET	443	49729	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.115782976 CET	443	49729	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.115840912 CET	49729	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.115869999 CET	49729	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.116492033 CET	49729	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.125734091 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.125771046 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.125822067 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.125834942 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.125848055 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.125850916 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.125866890 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.125874996 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.125895977 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.125900030 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.125917912 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.125936985 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.126015902 CET	443	49730	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.126355886 CET	443	49730	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.126673937 CET	443	49730	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.126713037 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.126739979 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.126769066 CET	49730	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.126776934 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.126779079 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.126804113 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.126816034 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.126830101 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.126841068 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.126868010 CET	443	49730	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.126883030 CET	49731	443	192.168.2.5	104.16.19.94

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 17:57:44.126904011 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.126908064 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.126945019 CET	49730	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.126950979 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.126960039 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.126987934 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.127001047 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.127013922 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.127032995 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.127051115 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.127054930 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.127075911 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.127104998 CET	443	49731	104.16.19.94	192.168.2.5
Jan 27, 2021 17:57:44.127115011 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.127155066 CET	49731	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.127382040 CET	49730	443	192.168.2.5	104.16.19.94
Jan 27, 2021 17:57:44.149719000 CET	443	49732	198.54.115.249	192.168.2.5
Jan 27, 2021 17:57:44.149888992 CET	443	49733	198.54.115.249	192.168.2.5
Jan 27, 2021 17:57:44.149986982 CET	49732	443	192.168.2.5	198.54.115.249

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 17:57:37.131891012 CET	65296	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:57:37.193311930 CET	53	65296	8.8.8.8	192.168.2.5
Jan 27, 2021 17:57:38.013611078 CET	63183	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:57:38.061681986 CET	53	63183	8.8.8.8	192.168.2.5
Jan 27, 2021 17:57:39.755141973 CET	60151	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:57:39.803185940 CET	53	60151	8.8.8.8	192.168.2.5
Jan 27, 2021 17:57:41.254218102 CET	56969	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:57:41.302097082 CET	53	56969	8.8.8.8	192.168.2.5
Jan 27, 2021 17:57:42.315231085 CET	55161	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:57:42.379410982 CET	53	55161	8.8.8.8	192.168.2.5
Jan 27, 2021 17:57:42.659456968 CET	54757	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:57:42.717443943 CET	53	54757	8.8.8.8	192.168.2.5
Jan 27, 2021 17:57:43.814822912 CET	49992	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:57:43.823338032 CET	60075	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:57:43.832113981 CET	55016	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:57:43.840373039 CET	64345	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:57:43.856520891 CET	57128	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:57:43.866960049 CET	54791	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:57:43.874203920 CET	53	60075	8.8.8.8	192.168.2.5
Jan 27, 2021 17:57:43.874294043 CET	53	49992	8.8.8.8	192.168.2.5
Jan 27, 2021 17:57:43.879650116 CET	50463	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:57:43.879951954 CET	53	55016	8.8.8.8	192.168.2.5
Jan 27, 2021 17:57:43.904467106 CET	53	57128	8.8.8.8	192.168.2.5
Jan 27, 2021 17:57:43.904495001 CET	53	64345	8.8.8.8	192.168.2.5
Jan 27, 2021 17:57:43.930387020 CET	53	50463	8.8.8.8	192.168.2.5
Jan 27, 2021 17:57:43.947732925 CET	53	54791	8.8.8.8	192.168.2.5
Jan 27, 2021 17:57:44.263641119 CET	50394	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:57:44.311922073 CET	53	50394	8.8.8.8	192.168.2.5
Jan 27, 2021 17:57:45.209455013 CET	58530	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:57:45.467606068 CET	53	58530	8.8.8.8	192.168.2.5
Jan 27, 2021 17:58:03.224899054 CET	53813	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:58:03.287715912 CET	53	53813	8.8.8.8	192.168.2.5
Jan 27, 2021 17:58:10.386693954 CET	63732	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:58:10.434776068 CET	53	63732	8.8.8.8	192.168.2.5
Jan 27, 2021 17:58:12.697875023 CET	57344	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:58:12.748442888 CET	53	57344	8.8.8.8	192.168.2.5
Jan 27, 2021 17:58:13.358254910 CET	54450	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:58:13.414895058 CET	53	54450	8.8.8.8	192.168.2.5
Jan 27, 2021 17:58:13.691150904 CET	57344	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:58:13.741957903 CET	53	57344	8.8.8.8	192.168.2.5
Jan 27, 2021 17:58:14.364392996 CET	54450	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 17:58:14.423142910 CET	53	54450	8.8.8.8	192.168.2.5
Jan 27, 2021 17:58:14.705290079 CET	57344	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:58:14.764821053 CET	53	57344	8.8.8.8	192.168.2.5
Jan 27, 2021 17:58:15.542515993 CET	54450	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:58:15.590928078 CET	53	54450	8.8.8.8	192.168.2.5
Jan 27, 2021 17:58:16.720776081 CET	57344	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:58:16.782279015 CET	53	57344	8.8.8.8	192.168.2.5
Jan 27, 2021 17:58:17.548965931 CET	54450	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:58:17.596824884 CET	53	54450	8.8.8.8	192.168.2.5
Jan 27, 2021 17:58:18.395212889 CET	59261	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:58:18.460874081 CET	53	59261	8.8.8.8	192.168.2.5
Jan 27, 2021 17:58:20.737557888 CET	57344	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:58:20.801601887 CET	53	57344	8.8.8.8	192.168.2.5
Jan 27, 2021 17:58:21.564897060 CET	54450	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:58:21.623965025 CET	53	54450	8.8.8.8	192.168.2.5
Jan 27, 2021 17:58:27.274749041 CET	57151	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:58:27.332873106 CET	53	57151	8.8.8.8	192.168.2.5
Jan 27, 2021 17:58:31.381330967 CET	59413	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:58:31.439366102 CET	53	59413	8.8.8.8	192.168.2.5
Jan 27, 2021 17:58:35.379731894 CET	60516	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:58:35.454655886 CET	53	60516	8.8.8.8	192.168.2.5
Jan 27, 2021 17:59:11.911361933 CET	51649	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:59:11.959177971 CET	53	51649	8.8.8.8	192.168.2.5
Jan 27, 2021 17:59:12.696932077 CET	65086	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:59:12.760945082 CET	53	65086	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 17:57:43.823338032 CET	192.168.2.5	8.8.8.8	0xa21e	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jan 27, 2021 17:57:43.832113981 CET	192.168.2.5	8.8.8.8	0x567	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Jan 27, 2021 17:57:43.856520891 CET	192.168.2.5	8.8.8.8	0x70cb	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Jan 27, 2021 17:57:43.866960049 CET	192.168.2.5	8.8.8.8	0xc5d6	Standard query (0)	app.forexliteoptions.com	A (IP address)	IN (0x0001)
Jan 27, 2021 17:57:43.879650116 CET	192.168.2.5	8.8.8.8	0x5f47	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jan 27, 2021 17:57:44.263641119 CET	192.168.2.5	8.8.8.8	0xed97	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Jan 27, 2021 17:57:45.209455013 CET	192.168.2.5	8.8.8.8	0x9506	Standard query (0)	www.stratexe.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 17:57:43.874203920 CET	8.8.8.8	192.168.2.5	0xa21e	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 17:57:43.879951954 CET	8.8.8.8	192.168.2.5	0x567	No error (0)	maxcdn.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 17:57:43.904467106 CET	8.8.8.8	192.168.2.5	0x70cb	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 17:57:43.930387020 CET	8.8.8.8	192.168.2.5	0x5f47	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jan 27, 2021 17:57:43.930387020 CET	8.8.8.8	192.168.2.5	0x5f47	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jan 27, 2021 17:57:43.947732925 CET	8.8.8.8	192.168.2.5	0xc5d6	No error (0)	app.forexliteoptions.com		198.54.115.249	A (IP address)	IN (0x0001)
Jan 27, 2021 17:57:44.311922073 CET	8.8.8.8	192.168.2.5	0xed97	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 17:57:45.467606068 CET	8.8.8.8	192.168.2.5	0x9506	No error (0)	www.stratexe.net		154.0.175.244	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
Jan 27, 2021 17:57:44.016836882 CET	104.16.19.94	443	192.168.2.5	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	Thu Oct 21 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=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		
Jan 27, 2021 17:57:44.017345905 CET	104.16.19.94	443	192.168.2.5	49730	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	Thu Oct 21 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=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		
Jan 27, 2021 17:57:44.025662899 CET	104.16.19.94	443	192.168.2.5	49731	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	Thu Oct 21 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=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		
Jan 27, 2021 17:57:44.349901915 CET	198.54.115.249	443	192.168.2.5	49732	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		

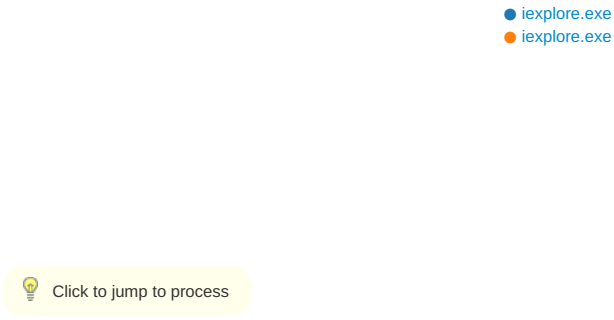
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 17:57:44.353200912 CET	198.54.115.249	443	192.168.2.5	49733	CN=app.forexliteoptions.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, 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		
Jan 27, 2021 17:57:45.925944090 CET	154.0.175.244	443	192.168.2.5	49736	CN=stratexe.net CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sat Dec 05 01:00:00 CET 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sat Mar 06 00:59:59 CET 2021 Sun May 18 01:59:59 CEST 2025 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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jan 27, 2021 17:57:45.931947947 CET	154.0.175.244	443	192.168.2.5	49737	CN=stratexe.net CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sat Dec 05 01:00:00 CET 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sat Mar 06 00:59:59 CET 2021 Sun May 18 01:59:59 CEST 2025 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 2076 Parent PID: 792

General

Start time:	17:57:42
Start date:	27/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff700600000
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	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: 4668 Parent PID: 2076

General

Start time:	17:57:42
Start date:	27/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2076 CREDAT:17410 /prefetch:2
Imagebase:	0xb10000
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