ID: 435311
Sample Name: ATT00001.htm
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 11:59:54
Date: 16/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

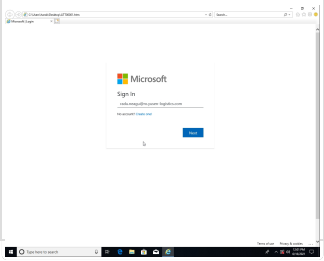
Windows Analysis Report ATT00001.htm

Overview

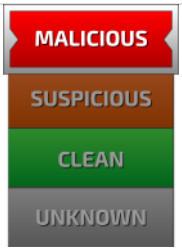
General Information

Sample Name:	ATT00001.htm
Analysis ID:	435311
MD5:	9bf6e3f48d1bb59..
SHA1:	250a41007b2e84..
SHA256:	3812cddabc0248..
Infos:	

Most interesting Screenshot:



Detection



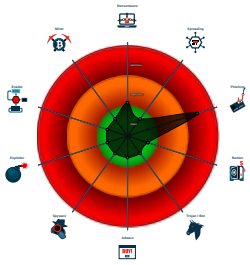
HTMLPhisher

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

Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- 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…

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 1304 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6116 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1304 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
ATT00001.htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

Phishing:

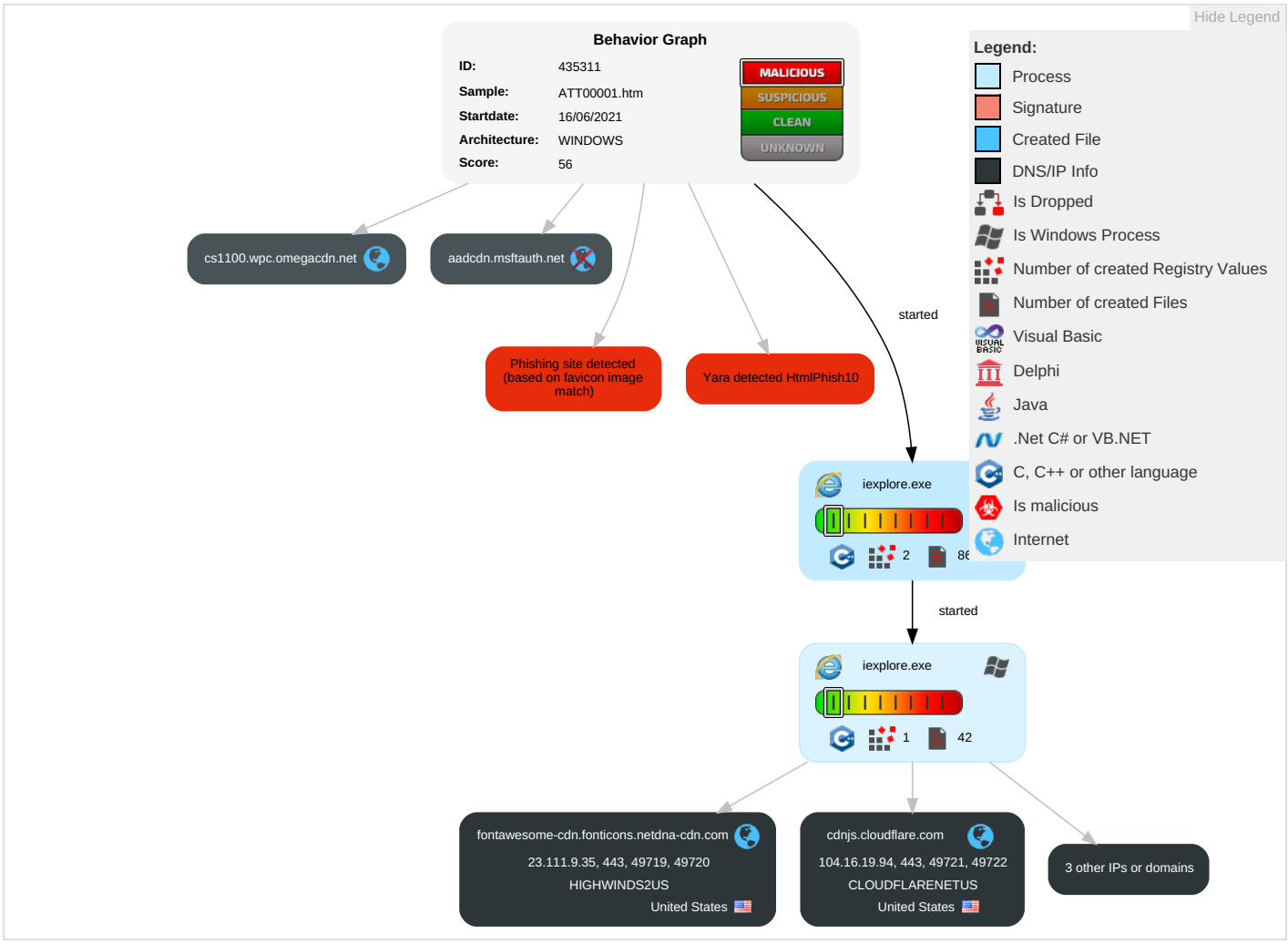
Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

Mitre Att&ck Matrix

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

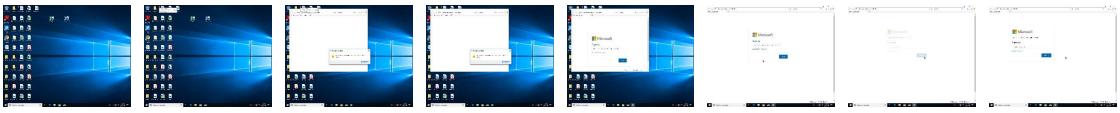
Behavior Graph

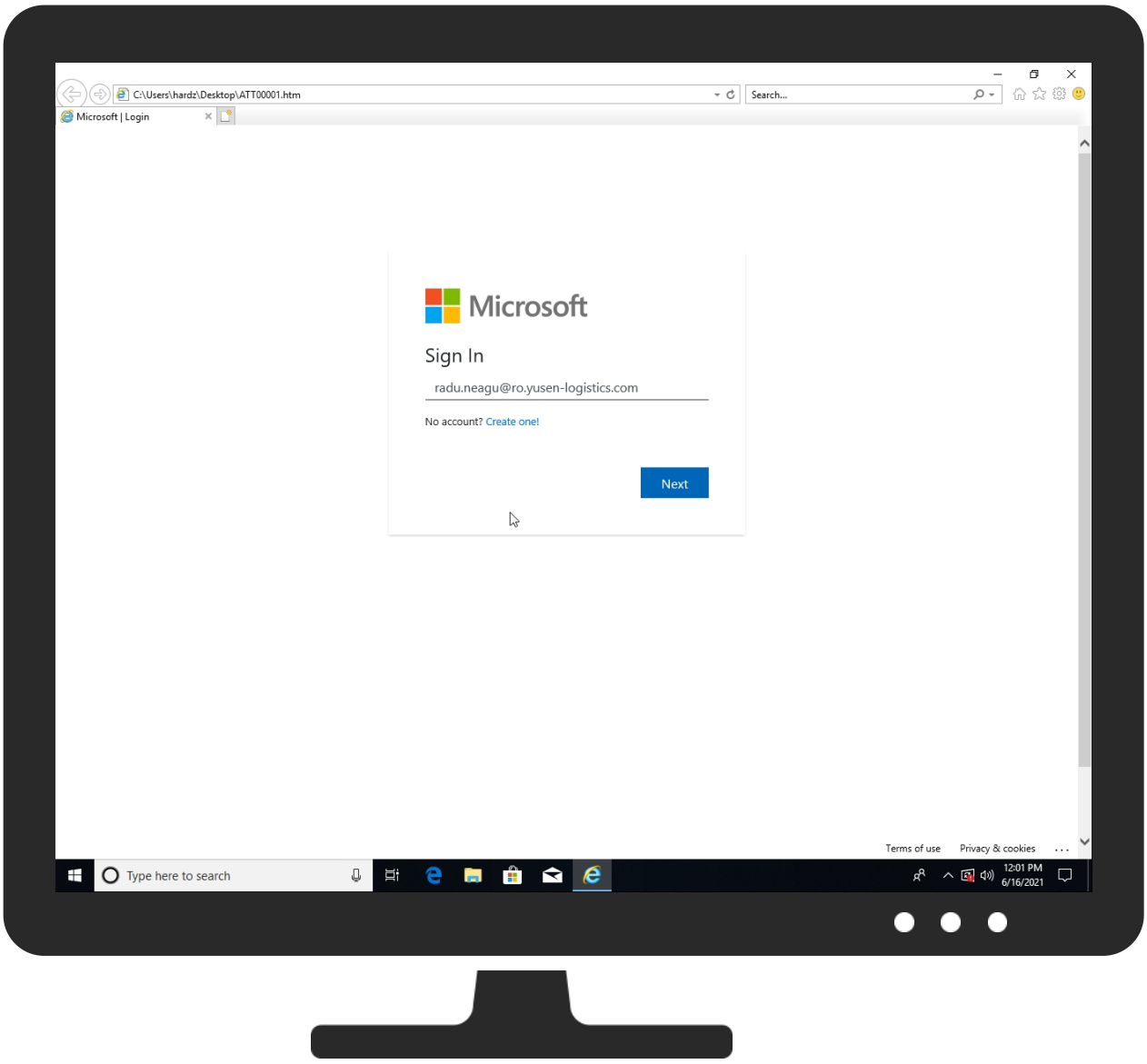


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://promisesaplus.com/#point-75	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-75	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-75	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-64	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-64	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-64	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-61	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-61	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-61	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-59	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-59	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-59	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-57	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-57	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-57	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-54	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-54	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-54	0%	URL Reputation	safe	
http://https://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://www.formtrap.com/enterprise/v8.0/manuals/en/images/fax_erp_1.gif	0%	Avira URL Cloud	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-48	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-48	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-48	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cs1100.wpc.omegacdn.net	152.199.23.37	true	false		unknown
cdnjs.cloudflare.com	104.16.19.94	true	false		high
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
fontawesome-cdn.fonticons.netdna-cdn.com	23.111.9.35	true	false		high
use.fontawesome.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/ATT00001.htm	true		low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.111.9.35	fontawesome-cdn.fonticons.netdna-cdn.com	United States		33438	HIGHWINDS2US	false
104.18.10.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	435311
Start date:	16.06.2021
Start time:	11:59:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ATT00001.htm
Cookbook file name:	defaultwindowshtmlcookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	26
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.winHTM@3/24@5/3
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .htm
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.111.9.35	http://1minutemarketing.net/	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://www.visioncraftng.com/wp-admin/paclm/aTOOClFPHUo66z	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://giftbuying411.com/wp-includes/64358352543832/1xd5izerfl-00002/	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://www.00rcasey.sebelt.com/?VGH=cmNhc2V5QGNnc2luYy5jb20=	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://www.00dhoy.sebelt.com/?VGH=ZGhveUBjZ3NpbmMuY2E=	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://casehunter.com.br	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://alaksir.com/Scripts/TW6LJpx/	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://azetta.org/Manage-AbsaOnlineBanking-httpsib.absa.co.zaabsa-onlinelogin.jsp-Logon-AbsaExpress/~AbsaOnline%206-1.htm	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://bluetechprism.com/css/9zWF1bV_EzUmPytyJH5nFH6_sector/individual_n8i69k9xbanwxg_cnav2o/549242_o6OPbP/	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://magecart.net	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://https://protect-us.mimecast.com/s/uOyvC4xWr5FzL0Zyux-GUS?domain=t.yesware.com	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://https://telegra.ph/Notification-Checkpoin2020-07-12-2?fbclid=IwAR3CW1pVoB2bo4DBxz90-mn4s4lYZcDve12Q_Z31J30jf9ZtOUBqmdx9ZjE	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://bespokemerchandises.com	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://https://v.ht/5DsS	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://lavicentelopezcaferesto.com.ar/aquawestdubbo/prop/normal/	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://earningtipsbd.com/pn/Buy-Sell_Agreement_0786719_04272020.zip	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://https://onedrive.live.com/view.aspx?resid=1A4116533EC50398!1032&authkey=!AEhxS1cHS1VlwMY	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://www.8888scents.com/js/	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://sakshampharmaceuticals.com/wp-includes/wglyons.php?t=VHVlLCAxNCBBcHIgMjAyMCAyMjowMTMwMA==	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://rjsimmonscpa.com/colopeaks	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
104.18.10.207	6334-Hanglung.com.html	Get hash	malicious	Browse	
	VM_7213436750_06_14_2-2.html	Get hash	malicious	Browse	
	_VM0_03064853.HtM	Get hash	malicious	Browse	
	payload.html	Get hash	malicious	Browse	
	Evershedsnicea NDA file attach...htm	Get hash	malicious	Browse	
	7 #U039c#U0456#U0455#U0455#U0435d #U0441 #U0430II#U0455.htm	Get hash	malicious	Browse	
	The Village.html	Get hash	malicious	Browse	
	GoogleChrome6.8.10.apk	Get hash	malicious	Browse	
	#Ud83d#Udda8rocket.com 1208421(69-queue-2615.htm	Get hash	malicious	Browse	
	receipt620.htm	Get hash	malicious	Browse	
	Secured-Message_7634-7.html	Get hash	malicious	Browse	
	original phishing email.html	Get hash	malicious	Browse	
	Return-message4928.html	Get hash	malicious	Browse	
	_.html	Get hash	malicious	Browse	
	Sealant Specialists, Inc. Projects #2021-Proposal #19100.html	Get hash	malicious	Browse	
	PAID Invoice name@gmail.com.htm	Get hash	malicious	Browse	
	mal.html	Get hash	malicious	Browse	
	mal.html	Get hash	malicious	Browse	
	mal.html	Get hash	malicious	Browse	
	hwJn3new_fax-message.html	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdnjs.cloudflare.com	#Ud83d#Udd7b Missed Call Playback Recording.wav - +1 6917381022.htm	Get hash	malicious	Browse	• 104.16.18.94
	6334-Hanglung.com.html	Get hash	malicious	Browse	• 104.16.18.94
	(786) 412-4567-Hanglung.com.html	Get hash	malicious	Browse	• 104.16.18.94
	Untitled attachment 00005.htm	Get hash	malicious	Browse	• 104.16.18.94
	(786) 593-7170-Mriglobal.org.html	Get hash	malicious	Browse	• 104.16.18.94
	(786) 274-1357-Hartmann.info.html	Get hash	malicious	Browse	• 104.16.19.94
	VM64DGCRMN5XGK.htm	Get hash	malicious	Browse	• 104.16.18.94
	payload.html	Get hash	malicious	Browse	• 104.16.18.94
	Ref#Doc30504871 Wyg.htm	Get hash	malicious	Browse	• 104.16.18.94
	Evershedsnicea NDA file attach...htm	Get hash	malicious	Browse	• 104.16.18.94
	Check 57549.Html	Get hash	malicious	Browse	• 104.16.19.94

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	7 #U039c#U0456#U0455#U0455#U0435d #U0441 #U0430II#U0455.htm	Get hash	malicious	Browse	• 104.16.19.94
	#Ud83d#Udcde_#U25b6#Ufe0f.htm	Get hash	malicious	Browse	• 104.16.19.94
	wzdu53.exe	Get hash	malicious	Browse	• 104.16.19.94
	The Village.html	Get hash	malicious	Browse	• 104.16.19.94
	#Ud83d#Udcde VM_58490931 Recoding.wav - 20223 PM. htm.htm	Get hash	malicious	Browse	• 104.16.19.94
	#Ud83d#Udda8northerntrust.hscni.net 692233150-queue-7828.htm	Get hash	malicious	Browse	• 104.16.19.94
	2ff0174.dll	Get hash	malicious	Browse	• 104.16.18.94
	Paid INV for Robert.landis Khs-net.htm	Get hash	malicious	Browse	• 104.16.18.94
	06.08.21 Inv & AP Statement - Copy.htm	Get hash	malicious	Browse	• 104.16.18.94
cs1100.wpc.omegacdn.net	SwiftDocument.HTML	Get hash	malicious	Browse	• 152.199.23.37
	Untitled attachment 00005.htm	Get hash	malicious	Browse	• 152.199.23.37
	May Release Check #39733.html	Get hash	malicious	Browse	• 152.199.23.37
	ATT00005.htm	Get hash	malicious	Browse	• 152.199.23.37
	7 #U039c#U0456#U0455#U0455#U0435d #U0441 #U0430II#U0455.htm	Get hash	malicious	Browse	• 152.199.23.37
	Julie.randall Completed REFERRAL AGREEMENT 60926.html	Get hash	malicious	Browse	• 152.199.23.37
	06.08.21 Inv & AP Statement - Copy.htm	Get hash	malicious	Browse	• 152.199.23.37
	#Ud83d#Udda8rocket.com 1208421(69-queue-2615.htm	Get hash	malicious	Browse	• 152.199.23.37
	Xerox scan.html	Get hash	malicious	Browse	• 152.199.23.37
	Brett.sutton REFERRAL AGREEMENT 03, Jun 2021 3444.html	Get hash	malicious	Browse	• 152.199.23.37
	PAID Invoice name@gmail.com.htm	Get hash	malicious	Browse	• 152.199.23.37
	#U266b Audio_47920.wavv - - Copy.html	Get hash	malicious	Browse	• 152.199.23.37
	Code-701.html	Get hash	malicious	Browse	• 152.199.23.37
	Sait_Message.htm	Get hash	malicious	Browse	• 152.199.23.37
	Lingarogroup_Scan_item.htm	Get hash	malicious	Browse	• 152.199.23.37
	DOC597-597.htm	Get hash	malicious	Browse	• 152.199.23.37
	PAYMENT_COPY420.htm	Get hash	malicious	Browse	• 152.199.23.37
	DOCUMENT997.htm	Get hash	malicious	Browse	• 152.199.23.37
	_____eFaxing@@@@@@@@@@dot.gov.html	Get hash	malicious	Browse	• 152.199.23.37
	_____eFaxing@@@@@@@@@@dot.gov.html	Get hash	malicious	Browse	• 152.199.23.37

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HIGHWINDS2US	invoice_sh.html	Get hash	malicious	Browse	• 23.111.9.35
	Untitled attachment 00005.htm	Get hash	malicious	Browse	• 23.111.9.35
	Evershedsnicea NDA file attach...htm	Get hash	malicious	Browse	• 23.111.9.35
	Paid INV for Robert.landis Khs-net.htm	Get hash	malicious	Browse	• 23.111.9.35
	saturo[1].htm	Get hash	malicious	Browse	• 23.111.9.64
	9553d0dcdf7b666c65cb7d42c092927c8aeae349ef30a.exe	Get hash	malicious	Browse	• 23.111.9.38
	ATT11972.HTM	Get hash	malicious	Browse	• 23.111.9.35
	Remittance_Advice.html	Get hash	malicious	Browse	• 23.111.9.35
	Statement - Past Due.html	Get hash	malicious	Browse	• 23.111.9.35
	VoicePlayback for Mjsansegundo Hispasat.htm	Get hash	malicious	Browse	• 23.111.9.35
	Sait_Message.htm	Get hash	malicious	Browse	• 23.111.9.35
	DOC597-597.htm	Get hash	malicious	Browse	• 23.111.9.35
	P#&162382090.html	Get hash	malicious	Browse	• 23.111.9.35
	Arbella NDA file attach...htm	Get hash	malicious	Browse	• 23.111.9.35
	Synchronoss NDA file attach...htm	Get hash	malicious	Browse	• 23.111.9.35
	Securecloudplus NDA file attach...htm	Get hash	malicious	Browse	• 23.111.9.35
	1CblHRpv2T.exe	Get hash	malicious	Browse	• 94.31.29.250
	PAYMENT_COPY420.htm	Get hash	malicious	Browse	• 23.111.9.35
	DOCUMENT997.htm	Get hash	malicious	Browse	• 23.111.9.35
	AP-swiftcopylcbuaivf.htm	Get hash	malicious	Browse	• 23.111.9.35
CLOUDFLARENETUS	RFQ-BCM 03122020.exe	Get hash	malicious	Browse	• 172.67.193.107
	Aries.exe	Get hash	malicious	Browse	• 162.159.130.233
	TT0900090000090.exe	Get hash	malicious	Browse	• 104.21.19.200
	Poczta Polska Informacje o transakcjach2021.exe	Get hash	malicious	Browse	• 104.21.1.82
	#Ud83d#Udd7b Missed Call Playback Recording.wav - +1 6917381022.htm	Get hash	malicious	Browse	• 104.16.18.94

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	AdobeAcrobatProDC2021.005.20048#U4e2d#U6587#U76f4#U88c5#U7834#U89e3#U7248@2223_16081.exe	Get hash	malicious	Browse	• 104.20.185.68
	PO-006 dtd-15.06.2021.exe	Get hash	malicious	Browse	• 104.21.15.48
	#U65b0#U8a02#U55ae_WJO-001.pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Zalando_mail_14.exe	Get hash	malicious	Browse	• 104.21.19.200
	6334-Hanglung.com.html	Get hash	malicious	Browse	• 104.16.18.94
	SecuriteInfo.com.W32.AIDetect.malware1.3553.exe	Get hash	malicious	Browse	• 172.67.206.104
	TscZlF3lqk.exe	Get hash	malicious	Browse	• 104.21.69.75
	8ti0qjm60b.exe	Get hash	malicious	Browse	• 172.67.137.101
	arm_crypt.exe	Get hash	malicious	Browse	• 172.67.188.10
	yfr02XrveJ.exe	Get hash	malicious	Browse	• 172.67.129.162
	ePThje5TvU.exe	Get hash	malicious	Browse	• 1.0.0.1
	PO#006611.doc.exe	Get hash	malicious	Browse	• 23.227.38.74
	ccbf1853c703609eda36bc07ab8eb2faf692153b56ecf.exe	Get hash	malicious	Browse	• 104.21.10.13
	Minutes of Meeting.exe	Get hash	malicious	Browse	• 104.21.19.200
	Consigment Details_pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
CLOUDFLARENETUS	RFQ-BCM 03122020.exe	Get hash	malicious	Browse	• 172.67.193.107
	Aries.exe	Get hash	malicious	Browse	• 162.159.130.233
	TT0900090000090.exe	Get hash	malicious	Browse	• 104.21.19.200
	Poczta Polska Informacje o transakcjach2021.exe	Get hash	malicious	Browse	• 104.21.1.82
	#Ud83d#Udd7b Missed Call Playback Recording.wav - +1 6917381022.htm	Get hash	malicious	Browse	• 104.16.18.94
	AdobeAcrobatProDC2021.005.20048#U4e2d#U6587#U76f4#U88c5#U7834#U89e3#U7248@2223_16081.exe	Get hash	malicious	Browse	• 104.20.185.68
	PO-006 dtd-15.06.2021.exe	Get hash	malicious	Browse	• 104.21.15.48
	#U65b0#U8a02#U55ae_WJO-001.pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Zalando_mail_14.exe	Get hash	malicious	Browse	• 104.21.19.200
	6334-Hanglung.com.html	Get hash	malicious	Browse	• 104.16.18.94
	SecuriteInfo.com.W32.AIDetect.malware1.3553.exe	Get hash	malicious	Browse	• 172.67.206.104
	TscZlF3lqk.exe	Get hash	malicious	Browse	• 104.21.69.75
	8ti0qjm60b.exe	Get hash	malicious	Browse	• 172.67.137.101
	arm_crypt.exe	Get hash	malicious	Browse	• 172.67.188.10
	yfr02XrveJ.exe	Get hash	malicious	Browse	• 172.67.129.162
	ePThje5TvU.exe	Get hash	malicious	Browse	• 1.0.0.1
	PO#006611.doc.exe	Get hash	malicious	Browse	• 23.227.38.74
	ccbf1853c703609eda36bc07ab8eb2faf692153b56ecf.exe	Get hash	malicious	Browse	• 104.21.10.13
	Minutes of Meeting.exe	Get hash	malicious	Browse	• 104.21.19.200
	Consigment Details_pdf.exe	Get hash	malicious	Browse	• 104.21.19.200

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	#Ud83d#Udd7b Missed Call Playback Recording.wav - +1 6917381022.htm	Get hash	malicious	Browse	• 23.111.9.35 • 104.18.10.207 • 104.16.19.94
	SecuriteInfo.com.MachineLearning.Anomalous.100.7906.exe	Get hash	malicious	Browse	• 23.111.9.35 • 104.18.10.207 • 104.16.19.94
	6334-Hanglung.com.html	Get hash	malicious	Browse	• 23.111.9.35 • 104.18.10.207 • 104.16.19.94
	Carole Gravelle's-Protected-Fax.htm	Get hash	malicious	Browse	• 23.111.9.35 • 104.18.10.207 • 104.16.19.94
	7#U1d05.html	Get hash	malicious	Browse	• 23.111.9.35 • 104.18.10.207 • 104.16.19.94
	Maryse Morin's-Protected-Fax.htm	Get hash	malicious	Browse	• 23.111.9.35 • 104.18.10.207 • 104.16.19.94
	HETZ.dll	Get hash	malicious	Browse	• 23.111.9.35 • 104.18.10.207 • 104.16.19.94
	HETZ.dll	Get hash	malicious	Browse	• 23.111.9.35 • 104.18.10.207 • 104.16.19.94
	VM_5823_05_24_2-2.html	Get hash	malicious	Browse	• 23.111.9.35 • 104.18.10.207 • 104.16.19.94

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SwiftDocument.HTML	Get hash	malicious	Browse	• 23.111.9.35 • 104.18.10.207 • 104.16.19.94
	I58yKFGZO4.exe	Get hash	malicious	Browse	• 23.111.9.35 • 104.18.10.207 • 104.16.19.94
	YiIS9HvO21.dll	Get hash	malicious	Browse	• 23.111.9.35 • 104.18.10.207 • 104.16.19.94
	1hIvIzTHG5.dll	Get hash	malicious	Browse	• 23.111.9.35 • 104.18.10.207 • 104.16.19.94
	xl7FJ4h7YS.dll	Get hash	malicious	Browse	• 23.111.9.35 • 104.18.10.207 • 104.16.19.94
	xDxD5fLpPC.dll	Get hash	malicious	Browse	• 23.111.9.35 • 104.18.10.207 • 104.16.19.94
	YiIS9HvO21.dll	Get hash	malicious	Browse	• 23.111.9.35 • 104.18.10.207 • 104.16.19.94
	AQvfg6cfsH.dll	Get hash	malicious	Browse	• 23.111.9.35 • 104.18.10.207 • 104.16.19.94
	1hIvIzTHG5.dll	Get hash	malicious	Browse	• 23.111.9.35 • 104.18.10.207 • 104.16.19.94
	0WX1X0cxwl.dll	Get hash	malicious	Browse	• 23.111.9.35 • 104.18.10.207 • 104.16.19.94
	34EH2vRFeU.dll	Get hash	malicious	Browse	• 23.111.9.35 • 104.18.10.207 • 104.16.19.94

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{25CEEA85-CED5-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33368
Entropy (8bit):	1.8753613444203268
Encrypted:	false
SSDEEP:	96:rqZBZS2kWIRtIkfI6FMIrL1ILIGI8tIHC3:rqZBZS2kW8tRfRFMW1M1ltgC3
MD5:	95A195DF8F3F32136D991230C5D09226
SHA1:	D05D258C2C8D658A6372110F725752F8CDD6A68E
SHA-256:	24C0A68DF687703F46E1A2369FE3EF90AC0D856C8FED9EA2C67E3D19C71B9528
SHA-512:	9504B0B3658332D98924BF91B9B9AA43306981276A87986C36780723B762003393975ACA682B9180F0F612C0B17A0D238477012DCD81EB4AD30EBCC3B72081E8
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\{25CEEA87-CED5-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28256
Entropy (8bit):	1.9179581117356852
Encrypted:	false
SSDEEP:	192:r8ZHQI6SkUj1I821GGW1QM1MYLZrLXD2Nr:r8wTLGYwvnxDDM
MD5:	7E32657CAC3BC79135E29A161D1E74C2

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{25CEEA87-CED5-11EB-90E4-ECF4BB862DED}.dat	
SHA1:	27ED06189E8944933A63BC8E10F0D9166C5C7B56
SHA-256:	B2D725A61B2C00FBAC3861D288354EA7458777846F2CB28C631C6C8EB96F1B4A
SHA-512:	0C86767C27593A8DA994DEA7A0F6975CD92A12E0A69C9C301F52A1E76762614408BA681B9F679D589AD6CF1729E1AC83AC7DF0873718B154AC7EFC0B8534CEC
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\{2E41C076-CED5-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5652290118302148
Encrypted:	false
SSDEEP:	48:IwuGcprcGwpa9G4pQxGrapbSCGQpKGcG7HpRGjTGIpG:ryZUQ/6BBSKAwTCA
MD5:	494A9973410A62094E72961FC4598E76
SHA1:	57C3C1161110A5B869D331A45432BBA6FBCE01C3
SHA-256:	3E730F1547355DAB3EE709304A0C5169536C7FFAD0841AE143AF63E3667220D4
SHA-512:	A0377E3FE7C67ED295D8D4E719CDDC32E0679A323FA117489D38FAF9692C3A8653EE7CA93D57A93D12422A054241657BB0F37652E46140368379D0FB285D3E7F
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):	5.053930151539948
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEj4l4xnWimI002EtM3MHdNMNxOEj4l4xnWimI00ObVbkEtMb:2d6NxOh+xSZHKd6NxOh+xSZ76b
MD5:	0C8D4907F800D44550452D06C640C75D
SHA1:	B247DB244814804E7C279B69663280C39D2F2E8A
SHA-256:	C41604B7F5A1BFE1BEE5D39624C3F889DABB3E5B81B8804AF05F017B44370304
SHA-512:	F241908B157B547B43C78581FFE1D4E6DF28EFE70A3778BC15F02D41CDE479DEB3B8EB23BE6EBA5C302E11BB496FAB70CF1169D5256E51C535D6AF992179AE F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xff3fc10d,0x01d762e1</date><accdate>0xff3fc10d,0x01d762e1</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>0xff3fc10d,0x01d762e1</date><accdate>0xff3fc10d,0x01d762e1</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):	5.091778256268012
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2k/EdExnWimI002EtM3MHdNMNxe2k/EdExnWimI00Obkak6EtMb:2d6NxrYSZHKd6NxrYSZ7Aa7b
MD5:	3C24A21818F0D0B4925C18BCA1941A57
SHA1:	BB5EC4C23DAD2F917F14CA56D1BEC5F44592CC36
SHA-256:	BFFDFFDD2CFA456457557A1C7AC649317C3FA60CFA2AD24AD9237A33D6DABFF5
SHA-512:	EFC1567F295DCDC7D1020B9FFD6F5A98704816C6460CD231F0BB5C82EAD2EAB5CDBCF5FDF3DE04EF7D99825F7B4D09DD2E991B143AEE0AB115AD79E1617A/ 169
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xff2f10bf,0x01d762e1</date><accdate>0xff2f10bf,0x01d762e1</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>0xff2f10bf,0x01d762e1</date><accdate>0xff2f10bf,0x01d762e1</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):	5.073018939339753
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLj4l4xnWimI002EtM3MHdNMNxvLj4l4xnWimI00ObmZEtMb:2d6NxvA+xSZHKd6NxvA+xSZ7mb
MD5:	56A214A396E2C90E40BFF66E4D40C811
SHA1:	5A911ECB2284FFB42B6DB2C07F9E4C933C0C5091
SHA-256:	5AB1D1769AED4319229E15073D3946D39086D6F4BF7DC8EA1457472A3AFD6E4F
SHA-512:	EC0406C786AC70879AA435A095C9B556718029182BBF1EF79F977515AD775DBB5D6D3217B08A31FCF1BD332B93D379FF42A1D6536A26D0B07388EE3479A380CA
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xff3fc10d,0x01d762e1</date><accdate>0xff3fc10d,0x01d762e1</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>0xff3fc10d,0x01d762e1</date><accdate>0xff3fc10d,0x01d762e1</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):	5.120573989807422
Encrypted:	false
SSDEEP:	12:TMHdNMNxiDnWimI002EtM3MHdNMNxiDnWimI00Obd5EtMb:2d6Nx8SZHKd6Nx8SZ7Jjb
MD5:	B1C31DE0CA281A548DDD868BDC3EF862
SHA1:	9E7822B9D3FAC840B7B2EE59A24FEBBE5723EDAD
SHA-256:	1629696961EE46D32B505347146A5677DBA2F3D7C403ADA6E94928CD108C513D
SHA-512:	01CEE008EB41985623BC9057E2D7F92BA22FE89C2DFC01E49E2482CFF0FAF875FBFFEBFAE3E01422067D2767AAF79155EBFF8F4F555F6A2E5504BB848564BE70
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xff3899fa,0x01d762e1</date><accdate>0xff3899fa,0x01d762e1</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>0xff3899fa,0x01d762e1</date><accdate>0xff3899fa,0x01d762e1</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):	5.088692637903771
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwj4l4xnWimI002EtM3MHdNMNxhGwj4l4xnWimI00Ob8K075EtMb:2d6NxQN+xSZHKd6NxQN+xSZ7YKajb
MD5:	26B8A8645880354DC4E359FAC6BDE249
SHA1:	EC6AD2DF55F889426BF318B7E0FF9E2795487E08
SHA-256:	8E8F81D970DA19F22A7E05797D24DCDDC7AD8202890CDCEA26FDB1207E2DC506
SHA-512:	3F4312BCBFCB02C5AC74FA77B0B7DD73DA170D69BED9F54F4D31CC03AA84D39BE1465E342754087AF2878796AC74851F9020E6FBDA503FE40291A6E0CFBD23F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xff3fc10d,0x01d762e1</date><accdate>0xff3fc10d,0x01d762e1</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>0xff3fc10d,0x01d762e1</date><accdate>0xff3fc10d,0x01d762e1</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-6757900\msapplication.xml	

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):	5.1078895068794345
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nDnWimI002EtM3MHdNMNx0nDnWimI00ObxEtMb:2d6Nx0DSZHKd6Nx0DSZ7nb
MD5:	7D22B18B2F3C3A57B0436BCF39699067
SHA1:	8FD71150B0815646EEF50FF0A9FC8CD41114126C
SHA-256:	9E27E88381BA649890BCDBE3E849BDC3E1C461A309F0D5651FE7760DDF29DD12
SHA-512:	64B70E90DC11CE069569D74B3B02F8003C0C8FB19F090BD0039CEEAFF1EB4DD9C95AED32E1DA489679AC8F4D2BC620B51AD9D8823722D770DA0F54203810461
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xff3899fa,0x01d762e1</date><accdate>0xff3899fa,0x01d762e1</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>0xff3899fa,0x01d762e1</date><accdate>0xff3899fa,0x01d762e1</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):	5.145094940239635
Encrypted:	false
SSDEEP:	12:TMHdNMNxxDnWimI002EtM3MHdNMNxxDnWimI00Ob6Kq5EtMb:2d6NxVSZHKd6NxVSZ7ob
MD5:	A7AF53851833B26E8C5B099C6E15FAB7
SHA1:	8D94D3991F13171C860FB431D3009AFF3839F184
SHA-256:	07AE06E652ACAC2772040AF983022498756237BC621BE76EB5E9030854ADC66F
SHA-512:	D84E2CCFC8618D951182CCCAC898952B158F313E7FEA098320366DF19EE7026CA8C6094FD5AB3C407C01683D3B9BB2DF57FA1528E4D0423347018CBF6D815CC
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xff3899fa,0x01d762e1</date><accdate>0xff3899fa,0x01d762e1</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>0xff3899fa,0x01d762e1</date><accdate>0xff3899fa,0x01d762e1</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):	5.122350494292771
Encrypted:	false
SSDEEP:	12:TMHdNMNxcDnWimI002EtM3MHdNMNxcDnWimI00ObVEtMb:2d6Nx+SZHKd6Nx+SZ7Db
MD5:	65124B9E2679647E019340407E914AC6
SHA1:	B524622BEA2CE00A842D31F2E0C9CC4174473DD8
SHA-256:	74457A0906EBD98950DDD297DD70D9659917D251477CC37C516A286515055A80
SHA-512:	954D53AB61657604F6084E30F726289B666A302B8F2D30288F949C5D8B89A2258EC499044FCE02B365148BAC90A723652C1A9C88E8EE377F7D8373836693A7FF
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xff3899fa,0x01d762e1</date><accdate>0xff3899fa,0x01d762e1</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>0xff3899fa,0x01d762e1</date><accdate>0xff3899fa,0x01d762e1</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\pin20332743330\msapplication.xml	

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):	5.106150723071345
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnDnWimI002EtM3MHdNMNxfnDnWimI00Obe5EtMb:2d6NxLSZHKd6NxLSZ7ijb
MD5:	81E7482FCFC08CA6CACAE7B0C68B55D3
SHA1:	8BC63D480F978FB0DC7CCB7B107CD05E3378941D
SHA-256:	42800222F1D646C2A1848E684163A5B2C37FEBBD0478EEECBBF0E066AD225317
SHA-512:	C7F0594E5C2A95BE169675D0A2C9D6F8B7FB2B4349DF5440D7F4D277D9A177E89ECC8BF36C3C943E8FA1F39431F05AEF02FC7223177A28417CF9FCE9D81B76D
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xff3899fa,0x01d762e1</date><accdate>0xff3899fa,0x01d762e1</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>0xff3899fa,0x01d762e1</date><accdate>0xff3899fa,0x01d762e1</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\all[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	54641
Entropy (8bit):	4.712564291864468
Encrypted:	false
SSDEEP:	768:SuV31Uz1RPq4NvvU63HJYkQCZ/WMQyjJKp7CzsGnQzU:SuczrC4NnzHSBCkgu7cs1w
MD5:	251D28BD755F5269A4531DF8A81D5664
SHA1:	C0F035B41B23C6E8FAB735F618AA3CFF0897B4F9
SHA-256:	AFDC6BF2DE981FFD7D370B76F44E7580572F197EFBE214B9CFA4005D189D8EAE
SHA-512:	8111F411C21C6011644139DBA4EF24D1696C0F6D31E55CE384E0353A0F3E65402170C502BDDF803C3DF9149C371B31C03F77BE98FDBC61C0C9C55AFBE399681
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://use.fontawesome.com/releases/v5.7.0/css/all.css
Preview:	/*!. * Font Awesome Free 5.7.0 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */..fa,.fab,.fal,.far,.fas{-moz-osx-font-smoothing:grayscale;-webkit-font-smoothing:antialiased;display:inline-block;font-style:normal;font-variant:normal;text-rendering:auto;line-height:1}.fa-lg{font-size:1.33333em;line-height:.75em;vertical-align:-.0667em}.fa-xs{font-size:.75em}.fa-sm{font-size:.875em}.fa-1x{font-size:1em}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-6x{font-size:6em}.fa-7x{font-size:7em}.fa-8x{font-size:8em}.fa-9x{font-size:9em}.fa-10x{font-size:10em}.fa-fw{text-align:center;width:1.25em}.fa-ul{list-style-type:none;margin-left:2.5em;padding-left:0}.fa-ul>li{position:relative}.fa-li{left:-2em;position:absolute;text-align:center;width:2em;line-height:inherit}.fa-border{border:.08em solid #eee;border-radius:.1em;padding:.2em .25em .15em}.fa-pull-lef

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery-3.3.1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	271751
Entropy (8bit):	5.0685414131801165
Encrypted:	false
SSDEEP:	6144:+tah6/K+TCtlMhTze/RZcYmDizK8dB7alFys/WL/umH4N0lPfKu5AA11vrlY:9pZcYmDcHwFygmY1PfjAA1Br3
MD5:	6A07DA9FAE934BAF3F749E876BBFDD96
SHA1:	46A436EBA01C79ACDB225757ED80BF54BAD6416B
SHA-256:	D8AA24ECC6CECB1A60515BC093F1C9DA38A0392612D9AB8AE0F7F36E6EEE1FAD
SHA-512:	E525248B09A6FB4022244682892E67BBF64A3E875EB889DB43B0A24AB4A75077B5D5D26943CA382750D4FEBC3883193F3BE581A4660065B6FC7B5EC20C4A044B
Malicious:	false
IE Cache URL:	http://https://code.jquery.com/jquery-3.3.1.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery-3.3.1[1].js	
Preview:	/*!. * jQuery JavaScript Library v3.3.1. * https://jquery.com/. *. * Includes Sizzle.js. * https://sizzlejs.com/. *. * Copyright JS Foundation and other contributors. * Released under the MIT license. * https://jquery.org/license. *. * Date: 2018-01-20T17:24Z. */.(function(global, factory) {..."use strict";...if (typeof module === "object" && typeof module.exports === "object") {..../// For CommonJS and CommonJS-like environments where a proper `window`.../// is present, execute the factory and get jQuery..../// For environments that do not have a `window` with a `document`.../// (such as Node.js), expose a factory as module.exports..../// This accentuates the need for the creation of a real `window`..../// e.g. var jQuery = require("jquery")(window);.../// See ticket #14549 for more info....module.exports = global.document ?....factory(global, true) :....function(w) {.....if (!w.document) {......throw new Error("jQuery requires a window with a document");.....}.....return factor

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jquery-3.1.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	86709
Entropy (8bit):	5.367391365596119
Encrypted:	false
SSDEEP:	1536:9NhEyjjTikEJO4edXXe9J578go6MWXqcVhrLyB4Lw13sh2bzrl1+iuH7U3gBORDT:jxcq0hrLZwpsYbmzORDU8Cu5
MD5:	E071ABDA8FE61194711CFC2AB99FE104
SHA1:	F647A6D37DC4CA055CED3CF64BBC1F490070ACBA
SHA-256:	85556761A8800D14CED8FCD41A6B8B26BF012D44A318866C0D81A62092EFD9BF
SHA-512:	53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D69067E65
Malicious:	false
IE Cache URL:	http://https://code.jquery.com/jquery-3.1.1.min.js
Preview:	/*! jQuery v3.1.1 | (c) jQuery Foundation | jquery.org/license */.!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.1.1",r=function(a,b){return new r.fn.init(a,b)},s=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,t=/^-ms-/,u=/-([a-z])/g,v=function(a,b){return b.toUpperCase()};r.fn=r.prototype={jquery:q,constructor:r,length:0,toArray:function(){return f.call(this)},get:function(a){return null==a?f.call(this):a<0?this[a+this.length]:this[a]},pushStack:function(a){var b=r.merge(this.con

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jquery-3.2.1.slim.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	69597
Entropy (8bit):	5.369216080582935
Encrypted:	false
SSDEEP:	1536:qNhEyjjTikEJO4edXXe9J578go6MWX2xkjVe4c4j2ll2Ac7pK3F71QDU8CuT:Exc2yjq4j2uYnQDU8CuT
MD5:	5F48FC77CAC90C4778FA24EC9C57F37D
SHA1:	9E89D1515BC4C371B86F4CB1002FD8E377C1829F
SHA-256:	9365920887B11B33A3DC4BA28A0F93951F200341263E3B9CEFD384798E4BE398
SHA-512:	CAB8C4AFA1D8E3A8B7856EE29AE92566D44CEEAD70C8D533F2C98A976D77D0E1D314719B5C6A473789D8C6B21EBB4B89A6B0EC2E1C9C618FB1437EBC77D3A269
Malicious:	false
IE Cache URL:	http://https://code.jquery.com/jquery-3.2.1.slim.min.js
Preview:	/*! jQuery v3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_evalUrl,-event/ajax,-effects,-effects/Tween,-effects/animatedSelector | (c) JS Foundation and other contributors | jquery.org/license */.!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\popper.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	19188
Entropy (8bit):	5.212814407014048
Encrypted:	false
SSDEEP:	384:+CbuG4xGNoDic2UjKPafxwC5b/4xQviOJU7QzxzivDdE3pcGdjkd/9jt3B+Kb964:zb4xGmiJfaf7gxQvVU7eziv+cSjknZ3f
MD5:	70D3FDA195602FE8B75E0097EED74DDE
SHA1:	C3B977AA4B8DFB69D651E07015031D385DED964B
SHA-256:	A52F7AA54D7BCAAFA056EE0A050262DFC5694AE28DEE8B4CAC3429AF37FF0D66
SHA-512:	51AFFB5A8CFD2F93B473007F6987B19A0A1A0FB970DDD59EF45BD77A355D82ABBBD60468837A09823496411E797F05B1F962AE93C725ED4C00D514BA40269D1
Malicious:	false
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\popper.min[1].js	
Preview:	/*. Copyright (C) Federico Zivolo 2017. Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT).. */(function(e,t){'object'==typeof exports&&'undefined'!=typeof module?module.exports=t():'function'==typeof define&&define.amd?define(t):e.Popper=t()})(this,function(){'use strict';function e(e){return e&&'[object Function]'==={}.toString.call(e)}function t(e,t){if(1!==e.nodeType)return[];var o=getComputedStyle(e,null);return t?o[t]:o}function o(e){return'HTML'===e.nodeName?e:e.parentNode||e.host}function n(e){if(!e)return document.body;switch(e.nodeName){case'HTML':case'BODY':return e.ownerDocument.body;case'#document':return e.body;}var i=t(e),r=i.overflow,p=i.overflowX,s=i.overflowY;return /(auto|scroll)/.test(r+s+p)?e:n(o(e))}function r(e){var o=e&&e.offsetParent,i=o&&o.nodeName;return i&&'BODY'!==i&&'HTML'!==i?-1!==['TD','TABLE'].indexOf(o.nodeName)&&'static'===t(o,'position')?r(o):o:e?e.ownerDocument.documentElement:document.documentElement}functio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	144877
Entropy (8bit):	5.049937202697915
Encrypted:	false
SSDEEP:	1536:GcoqwrUPyDHU7c7TcDEBi82NcuSELL4d/+oENM6HN26Q:VoPgPard2oENM6HN26Q
MD5:	450FC463B8B1A349DF717056FBB3E078
SHA1:	895125A4522A3B10EE7ADA06EE6503587CBF95C5
SHA-256:	2C0F3DCFE93D7E380C290FE4AB838ED8CADFF1596D62697F5444BE460D1F876D
SHA-512:	93BF1ED5F6D8B34F53413A86EFD4A925D578C97ABC757EA871F3F46F340745E4126C48219D2E8040713605B64A9ECF7AD986AA8102F5EA5ECF9228801D962F5D
Malicious:	false
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors. * Copyright 2011-2018 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--orange:#fd7e14;--yellow:#ffc107;--green:#28a745;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--primary:#007bff;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;--warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoint-xl:1200px;--font-family-sans-serif:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol";--font-family-monospace:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monospace}*,::after,::before{box-sizing:border-box}html{font-family:sans

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\bootstrap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	48944
Entropy (8bit):	5.272507874206726
Encrypted:	false
SSDEEP:	768:9VG5R15WbHVKZrycEHSYro34CrSLB6WU/6DqBf4l1B:9VIRuo53XiwWTvl1B
MD5:	14D449EB8876FA55E1EF3C2CC52B0C17
SHA1:	A9545831803B1359CFEED47E3B4D6BAE68E40E99
SHA-256:	E7ED36CEEE5450B4243BBC35188AFABDFB4280C7C57597001DE0ED167299B01B
SHA-512:	00D9069B9BD29AD0DAA0503F341D67549CCE28E888E1AFFD1A2A45B64A4C1BC460D81CFC4751857F991F2F4FB3D2572FD97FCA651BA0C2B0255530209B182F2
Malicious:	false
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,n){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function s(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function r(){return(r=Object.assign||function(t){for(var e=1;e<arguments.length;e++){var n=arguments[e];for(var i in n)Object.prototype.hasOwnProperty.call(n,i)&&(t[i]=n[i])}return t}).apply(this,arguments)}e=e&&e.hasOwnProperty("default")?e.default:e,n=n&&n.hasOwnProp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	223
Entropy (8bit):	5.142612311542767
Encrypted:	false
SSDEEP:	6:0IFFDK+Q+56ZRWHMqh7izlpdRSRk68k3tg9EFNin:jFI+QO6ZRoMqt6p3Tk9g9CY
MD5:	72C5D331F2135E52DA2A95F7854049A3
SHA1:	572F349BB65758D377CCBAE434350507341ACD7B
SHA-256:	C3A12D7E8F6B2B1F5E4CD0C9938DFC79532AEF90802B424EE910093F156586DA
SHA-512:	9EA12CC277C9858524083FEBBE1A3E61FDECE5268F63B14C9FFAFE29396C7CCDB3B07BE10E829936BCCD8F3B9E39DCFA6BC4316F189E4CEA914F1D06916DB66B
Malicious:	false
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Archivo+Narrow&display=swap

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\css[1].css	
Preview:	@font-face {. font-family: 'Archivo Narrow';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/archivonarrow/v12/tss0ApVBdCYD5Q7hcxTE1ArZ0bbwiXo.woff) format('woff');.}.

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):	85578
Entropy (8bit):	5.366055229017455
Encrypted:	false
SSDEEP:	1536:EYE1JVoiB9JqZdXXe2pD3PgoIiulrUndZ6a4tfOR7WpfWBZ2BJda4w9W3qG9a986:v4J+OlfOhWppCW6G9a98Hr2
MD5:	2F6B11A7E914718E0290410E85366FE9
SHA1:	69BB69E25CA7D5EF0935317584E6153F3FD9A88C
SHA-256:	05B85D96F41FFF14D8F608DAD03AB71E2C1017C2DA0914D7C59291BAD7A54F8E
SHA-512:	0D40BCCAA59FEDECF7243D63B33C42592541D0330FEFC78EC81A4C6B9689922D5B211011CA4BE23AE22621CCE4C658F52A1552C92D7AC3615241EB640F8514I B
Malicious:	false
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js
Preview:	/*! jQuery v2.2.4 | (c) jQuery Foundation | jquery.org/license */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="2.2.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,function(b,c){return a.call

C:\Users\user\AppData\Local\Temp\~DF192AE3E5F933E55A.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.28899143559771645
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAOT:kBqoxxJhHWSVSEabO
MD5:	1EA0AB28A0087DC99C42F7A5D8503073
SHA1:	ED85F14D37BBAAA29FA7862E466A5FD23E9B0FA3
SHA-256:	9E8954AEDAD42CDFD5A647F28793694F746E1A01C1EA01C5AC448D0055331517
SHA-512:	A32413F9E8E4B05BBD523038E234B8D0ED6EE18CB81DBFCD498B0DB7D50AA45D52D182CC7FC125B0970D0DF15FD14E0EE85FE9506FA71BC4DB87A89F0B10D 8C7
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF789282AEF4B257BF.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13077
Entropy (8bit):	0.5113851330592678
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo3F9loV9lWovrZrdqs7g:kBqoI+gov9rdB8
MD5:	BD42A5DB3A8A22B949A83FDB6AA6783D
SHA1:	5179A68A04BE9245CEC8FDAB5F9C9B9426E4B597
SHA-256:	FB74EBBB8C0333CD447BA3281E84C8843111F5D98A97F4C68911826EFD2184FF
SHA-512:	84B93A1D6D5C7692FE51D238DAFC8E53AD7BD896B4AD54088AD084AB4965C0F204502E0419A201AF74951E5AF2400799A85A5FC4A433CCE8205E62E311BEF4A B
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFDFEF816A16CDB662.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data

C:\Users\user\AppData\Local\Temp\~DFDFEF816A16CDB662.TMP	
Category:	dropped
Size (bytes):	36017
Entropy (8bit):	0.6021065914430312
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+1V17151o1EI1EMLEn0jA+P+jAZKYzWV0:kBqoxKAuvScS+1V17151o1r1/LHKa
MD5:	C689DA77D55BAF0708002ACF94C1FC0B
SHA1:	2ACDE3E1BF8928BAFFBD5BD598CA1AEBD495152E
SHA-256:	BF84461F6349E95E6F8603BC91E080434285714EAFBBFED2FA2C867B378E6B94
SHA-512:	9422BF008ADDB62E5186DACDAE3CDD89BECCE027016931ADABE07E860A61D5E023DE66BFDE38F469AF3A4DC0E422DC1509E78FC7C4BDA3A5BA6C20B27A5(1FC1
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

General

File type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	5.988382254142374
TrID:	• HyperText Markup Language (31031/1) 34.85% • HyperText Markup Language (12001/1) 13.48% • HyperText Markup Language (12001/1) 13.48% • HyperText Markup Language (11501/1) 12.92% • HyperText Markup Language (11501/1) 12.92%
File name:	ATT00001.htm
File size:	25011
MD5:	9bf6e3f48d1bb59fc4e688d6cc3e8977
SHA1:	250a41007b2e846ddf2d4b2308784e35747b9cd5
SHA256:	3812cddabc02487974ccf6001f8672ccc3cd39627f4a1b8 1956d9e7359cc1441
SHA512:	a64fc9454b6b74bb74dd7b3f11e910c2b5236a72c112451 1d7307d166e0cebd3aa1d9878d2d4d3c414c07654abc5d 55fe127b9adf54ee61642c60806a36306cf
SSDEEP:	384:k0W8iX7NaTqdXxuZeEBiX7NaTqdX2QY5sbnSRh: Rj+haGxxuZeK+haGx2Qc
File Content Preview:	<script type="text/javascript">..var startTime = new Date ().getTime();..var loadTime = null;..alert("Your email acc ount %EMAIL% has been signed out, click ok to sign in. ");..</script>..<!doctype html>..<html lang="it">..<head>. . <script type="text/javasc

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 16, 2021 12:00:45.093916893 CEST	192.168.2.3	8.8.8.8	0x3691	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jun 16, 2021 12:00:45.106348038 CEST	192.168.2.3	8.8.8.8	0x7de5	Standard query (0)	maxcdn.boo tstrapcdn.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 16, 2021 12:00:45.187647104 CEST	192.168.2.3	8.8.8.8	0x62b4	Standard query (0)	use.fontawesome.com	A (IP address)	IN (0x0001)
Jun 16, 2021 12:00:45.200541019 CEST	192.168.2.3	8.8.8.8	0xe0f4	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jun 16, 2021 12:01:01.784018040 CEST	192.168.2.3	8.8.8.8	0x675c	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 16, 2021 12:00:45.144478083 CEST	8.8.8.8	192.168.2.3	0x3691	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 16, 2021 12:00:45.165026903 CEST	8.8.8.8	192.168.2.3	0x7de5	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Jun 16, 2021 12:00:45.165026903 CEST	8.8.8.8	192.168.2.3	0x7de5	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Jun 16, 2021 12:00:45.240484953 CEST	8.8.8.8	192.168.2.3	0x62b4	No error (0)	use.fontawesome.com	fontawesome-cdn.fonticons.netdna-cdn.com		CNAME (Canonical name)	IN (0x0001)
Jun 16, 2021 12:00:45.240484953 CEST	8.8.8.8	192.168.2.3	0x62b4	No error (0)	fontawesome-cdn.fonticons.netdna-cdn.com		23.111.9.35	A (IP address)	IN (0x0001)
Jun 16, 2021 12:00:45.261234999 CEST	8.8.8.8	192.168.2.3	0xe0f4	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jun 16, 2021 12:00:45.261234999 CEST	8.8.8.8	192.168.2.3	0xe0f4	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jun 16, 2021 12:01:01.840250015 CEST	8.8.8.8	192.168.2.3	0x675c	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jun 16, 2021 12:01:01.840250015 CEST	8.8.8.8	192.168.2.3	0x675c	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 16, 2021 12:00:45.286917925 CEST	104.18.10.207	443	192.168.2.3	49716	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, 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 Mar 01 01:00:00 CET 2021	Tue Mar 01 00:59:59 CET 2022	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		
Jun 16, 2021 12:00:45.289597988 CEST	104.18.10.207	443	192.168.2.3	49714	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, 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 Mar 01 01:00:00 CET 2021	Tue Mar 01 00:59:59 CET 2022	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
Jun 16, 2021 12:00:45.370943069 CEST	104.16.19.94	443	192.168.2.3	49722	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020	Thu Oct 21 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
						CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jun 16, 2021 12:00:45.383368969 CEST	104.16.19.94	443	192.168.2.3	49721	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020	Thu Oct 21 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
						CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jun 16, 2021 12:00:45.389333963 CEST	23.111.9.35	443	192.168.2.3	49720	CN=*.fontawesome.com, O=Fonticons Inc, L=Bentonville, ST=Arkansas, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 13 01:00:00 CET 2020	Wed Dec 15 00:59:59 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
							Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031		
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jun 16, 2021 12:00:45.395566940 CEST	23.111.9.35	443	192.168.2.3	49719	CN=*.fontawesome.com, O=Fonticons Inc, L=Bentonville, ST=Arkansas, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 13 01:00:00 CET 2020	Wed Dec 15 00:59:59 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
							Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031		
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 1304 Parent PID: 792

General

Start time:	12:00:42
Start date:	16/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff763ae0000
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

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 6116 Parent PID: 1304

General

Start time:	12:00:43
Start date:	16/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1304 CREDAT:17410 /prefetch:2
Imagebase:	0xc40000
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

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly