ID: 356261
Sample Name: One Note
shergott@vivaldicap.com.html
Cookbook: default.jbs
Time: 20:23:12
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

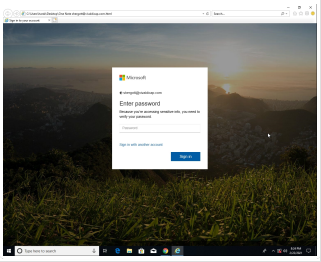
Analysis Report One Note shergott@vivaldicap.com.html

Overview

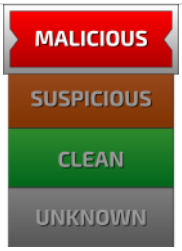
General Information

Sample Name:	One Note shergott@vivaldicap.com.html
Analysis ID:	356261
MD5:	6b9c5e9bfcf2518..
SHA1:	85c854dfc0e3ef1..
SHA256:	ffb4ba9437ffe8c4..

Most interesting Screenshot:



Detection



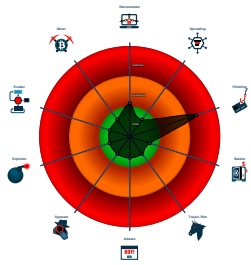
HTMLPhisher

Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish_10
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- None HTTPS page querying sensitiv…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6148 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6200 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6148 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

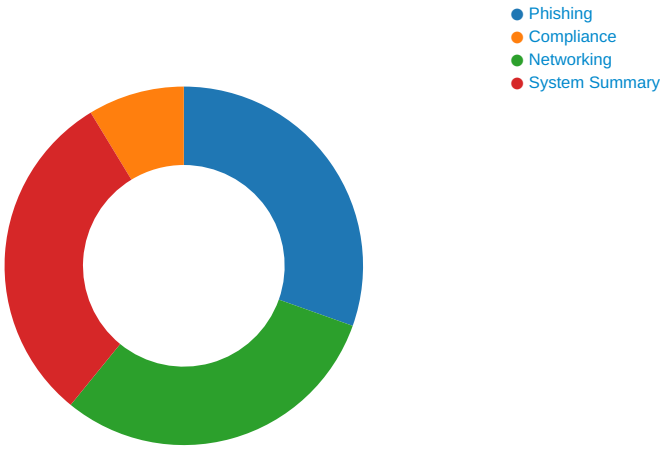
Initial Sample

Source	Rule	Description	Author	Strings
One Note shergott@vivaldicap.com.html	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:

Yara detected HtmlPhish_10

Phishing site detected (based on logo template match)

Compliance:

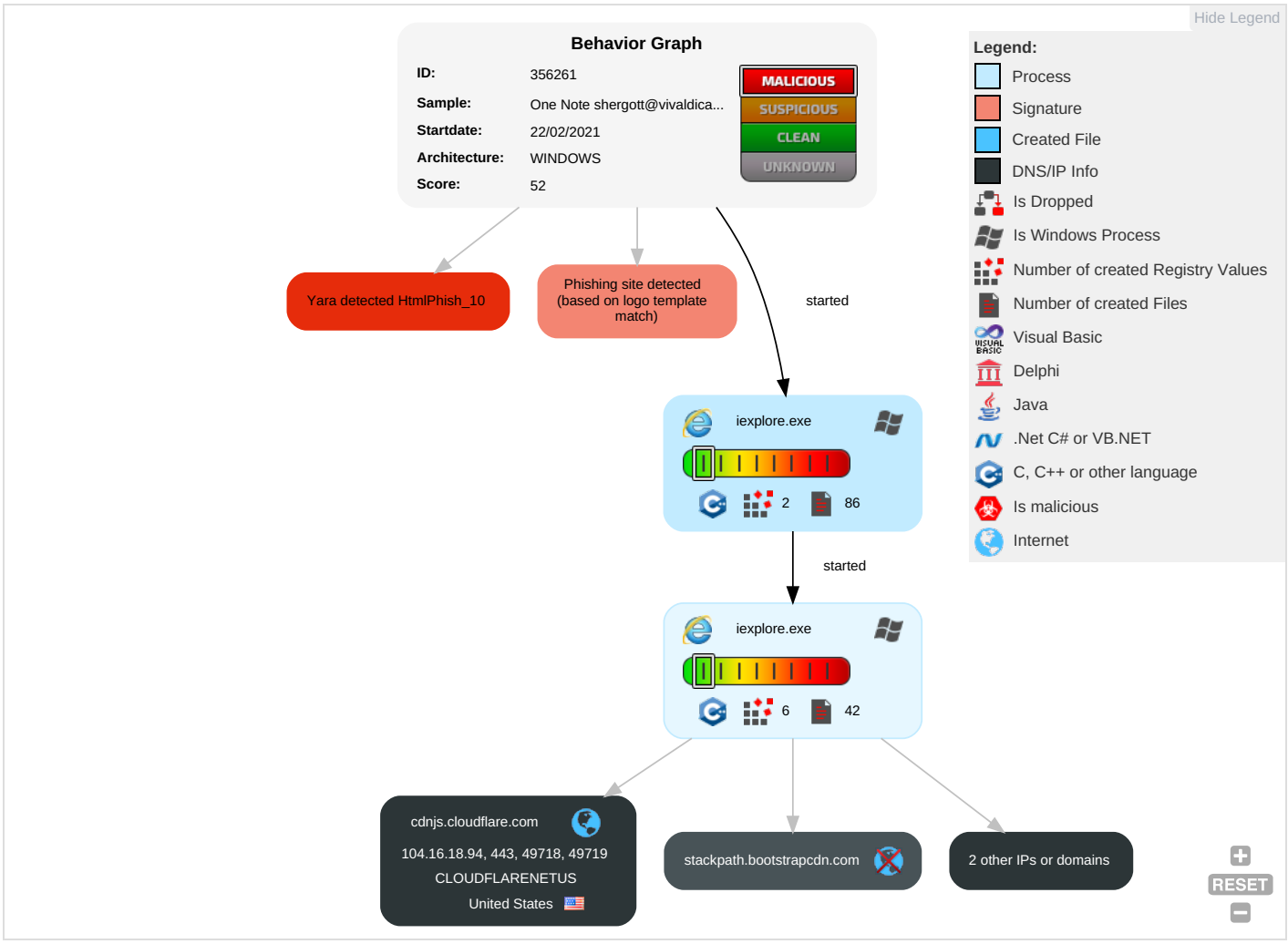
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Mitre Att&ck Matrix

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

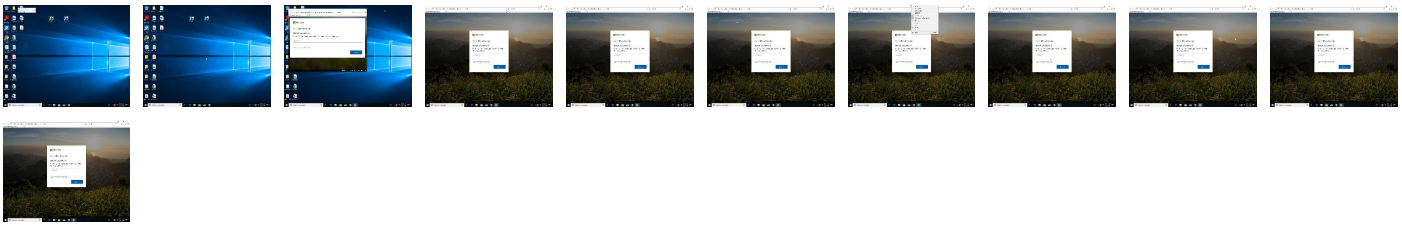
Behavior Graph

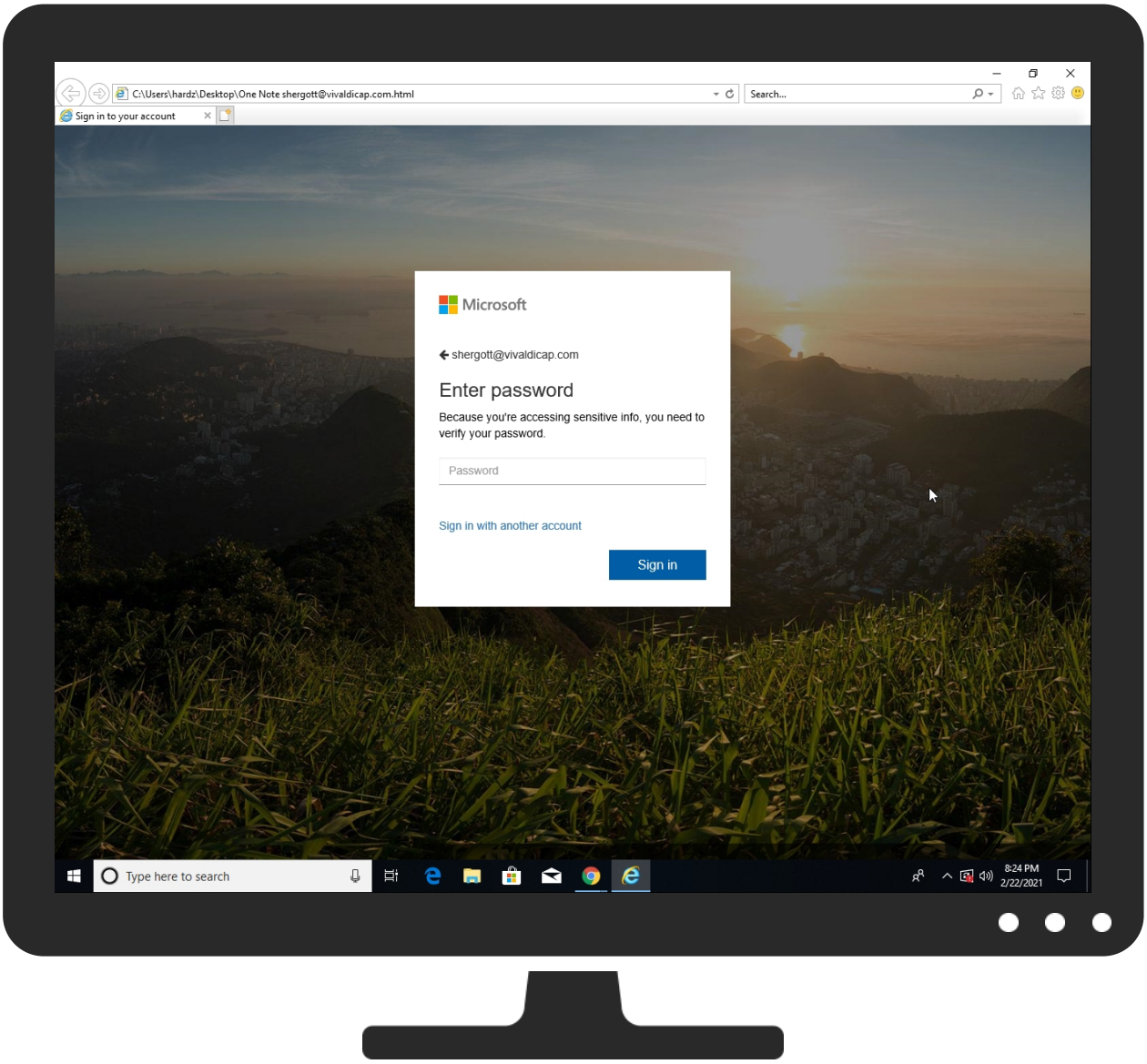


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://fontawesome.iohttp://fontawesome.iohttp://fontawesome.io/license/http://fontawesome.io/licens	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdnjs.cloudflare.com	104.16.18.94	true	false		high
stackpath.bootstrapcdn.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
maxcdn.bootstrapcdn.com	unknown	unknown	false		high

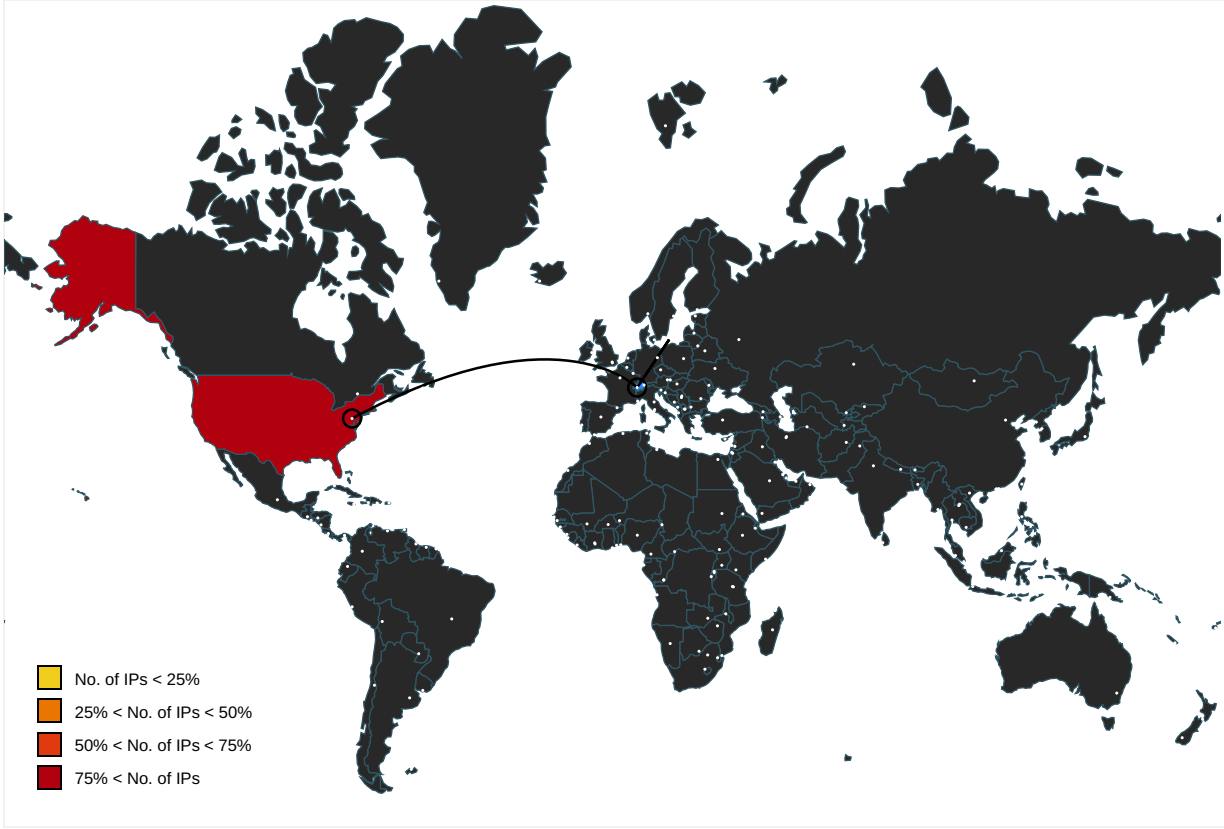
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/One%20Note%20shergott@vivaldicap.com.html	true		low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontawesome.io	fontawesome-webfont[1].eot.2.dr, font-awesome.min[1].css.2.dr	false		high
http://fontawesome.io/license/	fontawesome-webfont[1].eot.2.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.0/umd/popper.min.js	One Note shergott@vivaldicap.com.html	false		high
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css	One Note shergott@vivaldicap.com.html	false		high
http://fontawesome.iohttp://fontawesome.iohttp://fontawesome.io/license/http://fontawesome.io/licens	fontawesome-webfont[1].eot.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css	One Note shergott@vivaldicap.com.html	false		high
http://https://stackpath.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css	One Note shergott@vivaldicap.com.html	false		high
http://www.youtube.com/	msapplication.xml7.1.dr	false		high
http://https://code.jquery.com/jquery-3.1.1.min.js	One Note shergott@vivaldicap.com.html	false		high
http://getbootstrap.com)	bootstrap.min[1].js.2.dr	false	• Avira URL Cloud: safe	low
http://https://login.microsoftonline.com/jsdisabled	One Note shergott@vivaldicap.com.html	false		high
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[1].css.2.dr	false		high
http://https://code.jquery.com/jquery-3.3.1.slim.min.js	One Note shergott@vivaldicap.com.html	false		high
http://www.wikipedia.com/	msapplication.xml6.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.com/	msapplication.xml.1.dr	false		high
http://www.live.com/	msapplication.xml2.1.dr	false		high
http://opensource.org/licenses/MIT).	popper.min[1].js.2.dr	false		high
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://www.twitter.com/	msapplication.xml5.1.dr	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js	One Note shergott@vivaldicap.com.html	false		high
http://fontawesome.io/license	font-awesome.min[1].css.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.18.94	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356261
Start date:	22.02.2021
Start time:	20:23:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	One Note shergott@vivaldicap.com.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:	25
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:	mal52.phis.winHTML@3/23@4/1

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, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 51.104.139.180, 13.88.21.125, 104.43.193.48, 184.30.21.144, 88.221.62.148, 209.197.3.15, 209.197.3.24, 13.64.90.137, 23.57.80.111, 152.199.19.161, 51.11.168.160, 205.185.216.10, 205.185.216.42, 51.103.5.186, 92.122.213.247, 92.122.213.194, 20.54.26.129 • Excluded domains from analysis (whitelisted): cds.s5x3j6q5.hwcdn.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, go.microsoft.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ie9comview.vo.msecnd.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cds.j3z9t3p6.hwcdn.net, skypedataprdcolwus15.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net, cs9.wpc.v0cdn.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.16.18.94	http://https://bit.ly/35cYpiT	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://rva.fonotecanacional.gob.mx/preview-assets/css/smoothness/reports/chron_import.php?spent=1s0xppx5zxx96n&science=sun&round=hand	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bit.ly/2XaOiGR	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bitly.com/2Xaw8VA	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://j.mp/3rJBANn	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://www.rekmall.net/.well-known/acme-challenge/act_contactar2/admin_cat/mgc_chatbox/information-12/pspbrwse.php?sit=ervw1yb1atp20npd0&remember=quiet&feel=sleep	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://rassrochka.rusfishcom.ru/wp-snapshots/mailpage/information-66.php?sit=11kdh2bsq0r0z&bright=afraid&produce=sets	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bitly.com/3nmYKXc	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://j.mp/2URXSx8	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bit.ly/33I4Nht	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bit.ly/2Gwx0iC	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bit.ly/3jDHDOo	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://Kardanan.com	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/datamaps/0.5.8/datamaps.all.js

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdnjs.cloudflare.com	FAX-MESSAGE201636576736375362.hTMl	Get hash	malicious	Browse	• 104.16.18.94
	X1(1).xlsm	Get hash	malicious	Browse	• 104.16.19.94
	X1(1).xlsm	Get hash	malicious	Browse	• 104.16.18.94
	X1(1).xlsm	Get hash	malicious	Browse	• 104.16.18.94
	leaseplan-invoice-831008_xls2.HtMl	Get hash	malicious	Browse	• 104.16.18.94

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	CX2 RFQ.xlsm	Get hash	malicious	Browse	• 104.16.19.94
	CX2 RFQ.xlsm	Get hash	malicious	Browse	• 104.16.18.94
	CX2 RFQ.xlsm	Get hash	malicious	Browse	• 104.16.18.94
	C1.Qoute-Purequest Air Filtration Technologies (Pty) Ltd.xlsm	Get hash	malicious	Browse	• 104.16.18.94
	C1.Qoute-Purequest Air Filtration Technologies (Pty) Ltd.xlsm	Get hash	malicious	Browse	• 104.16.18.94
	C1.Qoute-Purequest Air Filtration Technologies (Pty) Ltd.xlsm	Get hash	malicious	Browse	• 104.16.18.94
	Deposit_50%PAYMENT TERM -PO09-excel.htm	Get hash	malicious	Browse	• 104.16.18.94
	OneNote rmos@dataflex-int.com.html	Get hash	malicious	Browse	• 104.16.19.94
	file.html	Get hash	malicious	Browse	• 104.16.19.94
	file.html	Get hash	malicious	Browse	• 104.16.19.94
	One Note keith.whitehead@lombard.co.uk.html	Get hash	malicious	Browse	• 104.16.19.94
	One Note tammy.ashwell@brewin.co.uk.html	Get hash	malicious	Browse	• 104.16.18.94
	barcelona-v-psg-liv-uefa-2021.html	Get hash	malicious	Browse	• 104.16.18.94
	Barcelona-v-PSG-0tv.html	Get hash	malicious	Browse	• 104.16.18.94
	One Note benjamin.lim@perpetual.com.au.html	Get hash	malicious	Browse	• 104.16.18.94

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	TT.exe	Get hash	malicious	Browse	• 172.67.172.17
	AWB-INVOICE_PDF.exe	Get hash	malicious	Browse	• 104.21.62.185
	purchase order 1.exe	Get hash	malicious	Browse	• 172.67.188.154
	telex transfer.exe	Get hash	malicious	Browse	• 172.67.188.154
	GPP.exe	Get hash	malicious	Browse	• 172.67.188.154
	DHL Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	#11032019 de investigaci#U00f3n de #U00f3rdenes,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Neue Bestellung_WJO-001, pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Halkbank_Ekstre_20210222_082357_541079.exe	Get hash	malicious	Browse	• 104.21.19.200
	swift payment.doc	Get hash	malicious	Browse	• 104.21.19.200
	FAX-MESSAGE201636576736375362.hTMl	Get hash	malicious	Browse	• 104.16.18.94
	Order_C3350191107102300.exe	Get hash	malicious	Browse	• 172.67.188.154
	SecuriteInfo.com.Trojan.Inject4.6572.17143.exe	Get hash	malicious	Browse	• 23.227.38.74
	SecuriteInfo.com.Trojan.Inject4.6572.13919.exe	Get hash	malicious	Browse	• 172.67.188.154
	Order.exe	Get hash	malicious	Browse	• 104.21.19.200
	upbck.xlsx	Get hash	malicious	Browse	• 104.22.1.232
	Invoices.exe	Get hash	malicious	Browse	• 172.67.172.17
	X1(1).xlsm	Get hash	malicious	Browse	• 104.16.19.94
	RFQ Manual Supersucker en Espaol.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	X1(1).xlsm	Get hash	malicious	Browse	• 104.16.18.94

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	FAX-MESSAGE201636576736375362.hTMl	Get hash	malicious	Browse	• 104.16.18.94
	message_zdm (2).html	Get hash	malicious	Browse	• 104.16.18.94
	Small Charities.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	leaseplan-invoice-831008_xls2.HtMl	Get hash	malicious	Browse	• 104.16.18.94
	7lM8HxwfAm.dll	Get hash	malicious	Browse	• 104.16.18.94
	LcA7GaqAXC.dll	Get hash	malicious	Browse	• 104.16.18.94
	4FHOFKHnX8.dll	Get hash	malicious	Browse	• 104.16.18.94
	5N5yxttthP.dll	Get hash	malicious	Browse	• 104.16.18.94
	vBKmtJ58Eo.dll	Get hash	malicious	Browse	• 104.16.18.94
	5293ea9467ea45e928620a5ed74440f5.exe	Get hash	malicious	Browse	• 104.16.18.94
	f1a14e6352036833f1c109e1bb2934f2.exe	Get hash	malicious	Browse	• 104.16.18.94
	Njs4kjnD5X.dll	Get hash	malicious	Browse	• 104.16.18.94
	Uiha1GUS7S.dll	Get hash	malicious	Browse	• 104.16.18.94
	SecuriteInfo.com.Mal.EncPk-APW.20360.dll	Get hash	malicious	Browse	• 104.16.18.94
	10.dll	Get hash	malicious	Browse	• 104.16.18.94
	iopjvdf.dll	Get hash	malicious	Browse	• 104.16.18.94
	d88e07467ddcf9e3b19fa972b9f000d1.exe	Get hash	malicious	Browse	• 104.16.18.94
	zP9r0Y0QaA.dll	Get hash	malicious	Browse	• 104.16.18.94
	kYHAeYQDFy.dll	Get hash	malicious	Browse	• 104.16.18.94
	AtxEaMk8Zr.dll	Get hash	malicious	Browse	• 104.16.18.94

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{F5371553-758E-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8587471974984615
Encrypted:	false
SSDEEP:	48:IwoGcprhGwpLWG/ap8eGIpccgGvnZpvcHGoeqp9cmGo4Fpmc+GWMc9cwGWicvcHJ:rcZ7ZU2uWc5tcXfcBFMc8c6cDfcfsX
MD5:	0E9A542A37F5CDD96E912C3C1E3F28E9
SHA1:	31F0B08F3602DC005E6BBB0A3685A53E0D3A7664
SHA-256:	B7A199C6B1B887D14B6774ED09F14DF0095AEF42454504E3BEC1C956191E3F94
SHA-512:	5E8AF34FE28E54FF77552B10427594CCD6CAFABF0B19793F2CFB15A70D6ED70AC3042BF889A42901524FC04EB7C272C55A78742871FF55F489EFC3B059614C54
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\{F5371555-758E-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28646
Entropy (8bit):	1.9696133935470732
Encrypted:	false
SSDEEP:	48:IwtGcprMGwpa8G4pQ0hGrapbSaGQpBvWGHHpc3TGUp8VWGzYpmUzGopVCasQWGSs:rzZkQc62BSij92BW8MYb8AseZNr
MD5:	44306EAA834658AB84CF29436B09614E
SHA1:	A37819938F8BC9AE67753FC67F1E2D64C869E342
SHA-256:	D4945FBED6B947E917DF4DACD6A64CAF4311EE4F968054554AFF9DF9CD1F89B6
SHA-512:	BD5A8A78DD4F4CFB8A46A763991970446292C1A6E0CDFD6454F927220BE180756EED4509BD900A31D8F12DCC306BFEDC734668CE996C77CE2B2C05243FA10CE
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\{F5371556-758E-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5649097639290814
Encrypted:	false
SSDEEP:	48:IwtGcprcGwpadG4pQKGrapbSuGQpK+1xG7HpR+1GTGIpG:rzZUQf68BSmA++T+UA
MD5:	187E845FD4984D7ABFC291639F647C78
SHA1:	7754FAAC83771D8C9691839AC0EA6C1FE10B9B9D
SHA-256:	E159A88311580E6A976E3E750A23C21548025284ACC52B18D39A7F7FEEEA1820
SHA-512:	258E8355F3C5E7143A5651AF9EDA4BD802AF4C50B87806F11B5EF5E4BDD214829964DBF13D65A1E5A42126263B445E5A7DAA213F075574C1D7D8E90B93989FE
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):	5.068204665551938
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEm4nWimI002EtM3MHdNMNxOEm4nWimI00ObVbkEtMb:2d6NxOWSZHKd6NxOWSZ76b
MD5:	8C79BD965644D7B3C9A871883E9716A7
SHA1:	7F8A0F5272C822630A3433F3B7A2C1006E432B66
SHA-256:	F5964DBF2A8FBF070037B7881A99EF8753DCC1E94BECDAEC282EAA1E8EC0CDF3
SHA-512:	9235B508872EC24BF98E2C4476E169662D8BDB0187886252A6F05BFC200DFC4481B4A8FDCA2C9A2BBEFD202409B8C855433BAACAD82DF46A514084A7973ADC 8
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xcaa7a5f8,0x01d7099b</date> accdate>0xcaa7a5f8,0x01d7099b</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>0xcaa7a5f8,0x01d7099b</date><accdate>0 xcaa7a5f8,0x01d7099b</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):	5.057338801916289
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kG4nWimI002EtM3MHdNMNxe2kG4nWimI00Obkak6EtMb:2d6Nxr2SZHKd6Nxr2SZ7Aa7b
MD5:	53D8F38EC416825F30536EB045806297
SHA1:	8ADE9650EEF5EF149F34176FD05A1ECA165F93F5
SHA-256:	F83D7BC1CF66E827A9AAD424F03262FFD18839EC7AF65788403B69E80AA711D0
SHA-512:	25588D3BC4AF4F13CBD798A1BC55DA0987EDBA861549A63C25517EABC6771504712FDE752AC6220C4011422F0BFFBBB640CF4FC02E1EDF3671884621D3F947D C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xca9e1c9c,0x01d7099b</date><a ccdate>0xca9e1c9c,0x01d7099b</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>0xca9e1c9c,0x01d7099b</date><a ccdate>0xca9e1c9c,0x01d7099b</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Am azon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.086147235145024
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLm4nWimI002EtM3MHdNMNxvLm4nWimI00ObmZEtMb:2d6Nxv/SZHKd6Nxv/SZ7mb
MD5:	9BB62540916380B87DA90DABCD34C6A4
SHA1:	F43A1DF117BF54DEA474A7946D162457C9CD585E
SHA-256:	925AB1CBFAB1C35AC1C51534968F5ACB86D0598948E5D86BDB3F5633F2861B51
SHA-512:	826C0C4172222CE44EEE83878156E5E762BE256A8DCA246CB443D31FC4184F3E01ACF61DAED871FC535C7327AE970DC17669A572115A36382ECCDDFBA357F6 3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xcaa7a5f8,0x01d7099b</date> <accdate>0xcaa7a5f8,0x01d7099b</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>0xcaa7a5f8,0x01d7099b</date><accda te>0xcaa7a5f8,0x01d7099b</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipe dia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Size (bytes):	647
Entropy (8bit):	5.083864036359874
Encrypted:	false
SSDEEP:	12:TMHdNMNxiA4nWimI002EtM3MHdNMNxiA4nWimI00Obd5EtMb:2d6NxSSZHKd6NxSSZ7Jjb
MD5:	8CB9A7646C6ECFE3F1CBEBEF4DBD3E69
SHA1:	C58AAFA581A71E30D8FAEEA318DCCB71955A8C83
SHA-256:	5105CC1B41AA8E470515B0C4D94473A9F4FB10DC94ACD47627C7253321DD0B16
SHA-512:	D84C5D59091CA2E348392CFCA0D246B33C59C10ED5BF0DE4F15744506E730B710C871BCE9D7959E8824D76B36CA531FC61BA47F6A34CF0B9712CF12AE20DE0D
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xcaa543aa,0x01d7099b</date><accdate>0xcaa543aa,0x01d7099b</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>0xcaa543aa,0x01d7099b</date><accdate>0xcaa543aa,0x01d7099b</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):	5.083327609465694
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwEtJ4nWimI002EtM3MHdNMNxhGwEtJ4nWimI00Ob8K075EtMb:2d6NxQ5tuSZHKd6NxQ5tuSZ7YKajb
MD5:	55A04FF4ADB63EE1F992402F7DCA0708
SHA1:	EC03CD170D299D92E1AD5F6145D26648EA87ACF3
SHA-256:	E40B79D2DA2BB9B8B219AE871B05675ECABAE9453783BB2AE85A2EE6DD668AE1
SHA-512:	0F35E03750BA3FF4EFBE4B811E7CD23FF8A80A32DB4AA5589D8FB0A2325BBAB1C257E6C838A44450E0853FC0101FBF497C728625CD76AD083B8049854E32713(
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xcaaa0833,0x01d7099b</date><accdate>0xcaaa0833,0x01d7099b</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>0xcaaa0833,0x01d7099b</date><accdate>0xcaaa0833,0x01d7099b</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):	5.071516857751467
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nA4nWimI002EtM3MHdNMNx0nA4nWimI00ObxEtMb:2d6Nx0ZSZHKd6Nx0ZSZ7nb
MD5:	09B663E522327276D936E48B2D2ABA90
SHA1:	C970334E13E73B767F00705FC2AE8FF7956EB815
SHA-256:	860029ABCE5171AC8B4BA171F52E5A1CF38F5C9486239DAF63CA4646506B8226
SHA-512:	93F595088E11FB33639EA2E6A622CBF15AFA940F0BEA6564716885FDA8DE1CD791C4AD5BC6BDE2F7614DF59F5949005829DC3154DEBDC46CBC7D10AE1FAAE5C8
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xcaa543aa,0x01d7099b</date><accdate>0xcaa543aa,0x01d7099b</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>0xcaa543aa,0x01d7099b</date><accdate>0xcaa543aa,0x01d7099b</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\pin202591677780\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):	5.108888629446093
Encrypted:	false
SSDEEP:	12:TMHdNMNxxA4nWimI002EtM3MHdNMNxxA4nWimI00Ob6Kq5EtMb:2d6NxrSZHKd6NxrSZ7ob

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
MD5:	203787AD80C5B5A48C00C0DA7946EBB1
SHA1:	4E0E08120AC2F0EF6EEF6A08832B87E1EDCA1329
SHA-256:	9343DDB5DD37C492E97290A9251D645D0E9969696D9D5EFF8D6766F7D57DC746
SHA-512:	C4F9BF38A9B1A9604E923FE3591BF3D0E806F59E40E37A297DCFCD49B24D2C287C9B6FD065B86E9E95E223F5EFB8F4A91D40C2916E8047C27A3BC1E624AB2E8
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xcaa543aa,0x01d7099b</date><accdate>0xcaa543aa,0x01d7099b</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>0xcaa543aa,0x01d7099b</date><accdate>0xcaa543aa,0x01d7099b</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):	5.086809285125789
Encrypted:	false
SSDEEP:	12:TMHdNMNxccbtbJ4nWimI002EtM3MHdNMNxccbtbJ4nWimI00ObVEtMb:2d6NxOSZHKd6NxOSZ7Db
MD5:	CA9CA125D05D7355EFB64E7700194C0B
SHA1:	88A54F36FB23025616B9C8999AB0EF22779C901C
SHA-256:	50383B2C13C41911E3DD3458D542DC2CA20A20AAAB7BE673EC503002FDD95705
SHA-512:	330A9FA568D53F940368FA3E1BD0ACBFBC7C63A6D616FF5AF3774F4FE9CDD2EBEDC89EF7280280064DCE53152E0842E3FFBB1C5D4374A4258C19209F7A2A2DD
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xcaa2e129,0x01d7099b</date><accdate>0xcaa2e129,0x01d7099b</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>0xcaa2e129,0x01d7099b</date><accdate>0xcaa2e129,0x01d7099b</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):	5.072536144041136
Encrypted:	false
SSDEEP:	12:TMHdNMNxfncbtbJ4nWimI002EtM3MHdNMNxfncbtbJ4nWimI00Obe5EtMb:2d6NxbSZHKd6NxbSZ7ijb
MD5:	3A6FADF0C8C049019853C08FA51D1668
SHA1:	86E6DBCC34362624B5F157A307DB7815F53FB82F
SHA-256:	392839E6C9D99578DE321313C1F3A3D1811DC8C0A26BCD539A024506E3372190
SHA-512:	81B7620475C1D287881DD319F028E09F89FEFFA8E3691DF2648206F9E8CE019919C17BD5DEF65B47630AB2A9B43E7F5138858E90CE71EA50B6171D7391E83938
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xcaa2e129,0x01d7099b</date><accdate>0xcaa2e129,0x01d7099b</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>0xcaa2e129,0x01d7099b</date><accdate>0xcaa2e129,0x01d7099b</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\font-awesome.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	31000
Entropy (8bit):	4.746143404849733
Encrypted:	false
SSDEEP:	384:wHu5yWeTUKW+KlkJ5de2UYDyVfwYUas2l8yQ/8dwmaU8G:wwlr+Klk3Yi+fwYUf2l8yQ/e9vf
MD5:	269550530CC127B6AA5A35925A7DE6CE
SHA1:	512C7D79033E3028A9BE61B540CF1A6870C896F8
SHA-256:	799AEB25CC0373FDEE0E1B1DB7AD6C2F6A0E058DFADAA3379689F583213190BD

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\font-awesome.min[1].css	
SHA-512:	49F4E24E55FA924FAA8AD7DEBE5FFB2E26D439E25696DF6B6F20E7F766B50EA58EC3DBD61B6305A1ACACD2C80E6E659ACCEE4140F885B9C9E71008E9001FBF4B
Malicious:	false
Reputation:	high, very likely benign file
IE Cache URL:	http://https://stackpath.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css
Preview:	/*!. * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */@font-face{font-family:'FontAwesome';src:url('../fonts/fontawesome-webfont.eot?v=4.7.0');src:url('../fonts/fontawesome-webfont.eot?#iefix&v=4.7.0') format('embedded-opentype'),url('../fonts/fontawesome-webfont.woff2?v=4.7.0') format('woff2'),url('../fonts/fontawesome-webfont.woff?v=4.7.0') format('woff'),url('../fonts/fontawesome-webfont.ttf?v=4.7.0') format('truetype'),url('../fonts/fontawesome-webfont.svg?v=4.7.0#fontawesomeregular') format('svg');font-weight:normal;font-style:normal}.fa{display:inline-block;font:normal normal normal 14px/1 FontAwesome;font-size:inherit;text-rendering:auto;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.fa-lg{font-size:1.33333333em;line-height:.75em;vertical-align:-15%}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-fw{width:1.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fontawesome-webfont[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), FontAwesome family
Category:	downloaded
Size (bytes):	165742
Entropy (8bit):	6.705073372195656
Encrypted:	false
SSDEEP:	3072:qbhEnD+IzsU9z9QJ6/P3Xe2iEiEPGFCMW1JVJG6wVTDsk6BmG6S1yKshojskO+b2:qenD+IzsU9z9QJ6/PO2FiEP2C/DVJG6I
MD5:	674F50D287A8C48DC19BA404D20FE713
SHA1:	D980C2CE873DC43AF460D4D572D441304499F400
SHA-256:	7BFCAB6DB99D5CFBF1705CA0536DDC78585432CC5FA41BBD7AD0F009033B2979
SHA-512:	C160D3D77E67EFF986043461693B2A831E1175F579490D7F0B411005EA81BD4F5850FF534F6721B727C002973F3F9027EA960FAC4317D37DB1D4CB53EC9D343A
Malicious:	false
IE Cache URL:	http://https://stackpath.bootstrapcdn.com/font-awesome/4.7.0/fonts/fontawesome-webfont.eot?
Preview:	n.....LP.....Yx.....F.o.n.t.A.w.e.s.o.m.e.....R.e.g.u.l.a.r...$.V.e.r.s.i.o.n. .4...7...0. .2.0.1.6.....F.o.n.t.A.w.e.s.o.m.e.....PFFTMk .G.....GDEF.....p... OS/2.2z@...X...`cmap..:.....gasp.....h....glyf...M.....L.head...-.....6hhea.....$hmtxEy.....loca...\.....maxp.,.....8... name....gh....post.....k.... u.....xY_.<.....3.2.....3.2.....'.....@.....i.....3.....3...s.....pyrs.@. ....p.....U..... .....]..... .....y...n.....2.....@..... ....z.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fontawesome-webfont[2].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), FontAwesome family
Category:	downloaded
Size (bytes):	165742
Entropy (8bit):	6.705073372195656
Encrypted:	false
SSDEEP:	3072:qbhEnD+IzsU9z9QJ6/P3Xe2iEiEPGFCMW1JVJG6wVTDsk6BmG6S1yKshojskO+b2:qenD+IzsU9z9QJ6/PO2FiEP2C/DVJG6I
MD5:	674F50D287A8C48DC19BA404D20FE713
SHA1:	D980C2CE873DC43AF460D4D572D441304499F400
SHA-256:	7BFCAB6DB99D5CFBF1705CA0536DDC78585432CC5FA41BBD7AD0F009033B2979
SHA-512:	C160D3D77E67EFF986043461693B2A831E1175F579490D7F0B411005EA81BD4F5850FF534F6721B727C002973F3F9027EA960FAC4317D37DB1D4CB53EC9D343A
Malicious:	false
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/fonts/fontawesome-webfont.eot?
Preview:	n.....LP.....Yx.....F.o.n.t.A.w.e.s.o.m.e.....R.e.g.u.l.a.r...$.V.e.r.s.i.o.n. .4...7...0. .2.0.1.6.....F.o.n.t.A.w.e.s.o.m.e.....PFFTMk .G.....GDEF.....p... OS/2.2z@...X...`cmap..:.....gasp.....h....glyf...M.....L.head...-.....6hhea.....$hmtxEy.....loca...\.....maxp.,.....8... name....gh....post.....k.... u.....xY_.<.....3.2.....3.2.....'.....@.....i.....3.....3...s.....pyrs.@. ....p.....U..... .....]..... .....y...n.....2.....@..... ....z.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	121200
Entropy (8bit):	5.0982146191887106
Encrypted:	false
SSDEEP:	768:Vy3Gxw/Vc/QWlJxtQOIuiHlq5mzI4X8OAduFKbv2ctg2Bd8JP7ecQVvH1FS:nw/a1fIuiHlq5mN8lDbNmPbh
MD5:	EC3BB52A00E176A7181D454DFFAEA219
SHA1:	6527D8BF3E1E9368BAB8C7B60F56BC01FA3AFD68
SHA-256:	F75E846CC83BD11432F4B1E21A45F31BC85283D11D372F7B19ACCD1BF6A2635C
SHA-512:	E8C5DAF01EAE68ED7C1E277A6E544C7AD108A0FA877FB531D6D9F2210769B7DA88E4E002C7B0BE3B72154EBF7CBF01A795C8342CE2DAD368BD6351E956195F8B
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bootstrap.min[1].css	
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\MEEXW4H4\bootstrap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	37045
Entropy (8bit):	5.174934618594778
Encrypted:	false
SSDEEP:	768:o2rGy27UwlNqMl95qNmCFejhqs8snmi+CSFXfbx8Gf3Zq7Q:Jg73zhq0GvbJ3ZKQ
MD5:	5869C96CC8F19086AEE625D670D741F9
SHA1:	430A443D74830FE9BE26EFCA431F448C1B3740F9
SHA-256:	53964478A7C634E8DAD34ECC303DD8048D00DCE4993906DE1BACF67F663486EF
SHA-512:	8B3B64A1BB2F9E329F02D4CD7479065630184EBAED942EE61A9FF9E1CE34C28C0EECB854458977815CF3704A8697FA8A5D096D2761F032B74B70D51DA3E37F4
Malicious:	false
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v3.3.7 (http://getbootstrap.com). * Copyright 2011-2016 Twitter, Inc.. * Licensed under the MIT license. */.if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery");+function(a){"use strict";var b=a.fn.jquery.split(" ")[0].split(".");if(b[0]<2&&b[1]<9||1==b[0]&&9==b[1]&&b[2]<1||b[0]>3)throw new Error("Bootstrap's JavaScript requires jQuery version 1.9.1 or higher, but lower than version 4")}(jQuery),+function(a){"use strict";function b(){var a=document.createElement("bootstrap"),b={WebkitTransition:"webkitTransitionEnd",MozTransition:"transitionend",OTransition:"oTransitionEnd otransitionend",transition:"transitionend"};for(var c in b)if(void 0!==a.style[c])return{end:b[c]};return!1}a.fn.emulateTransitionEnd=function(b){var c=!1,d=this;a(this).one("bsTransitionEnd",function(){c=!0});var e=function(){c||a(d).trigger(a.support.transition.end)};return setTimeout(e,b),this},a(function(){a.support.transition=b(),a.support.transition&&(a.event.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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\WJ8I2OL4\font-awesome[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	troff or preprocessor input, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	37414
Entropy (8bit):	4.82325822639402
Encrypted:	false
SSDEEP:	768:mmMtI+A4CSIDqvnI+YTBrFPvVrJjhiRAiiEL:mXtI+A4GDUI+Y9rpVljhiIEL
MD5:	C495654869785BC3DF60216616814AD1
SHA1:	0140952C64E3F2B74EF64E050F2FE86EAB6624C8
SHA-256:	36E0A7E08BEE65774168528938072C536437669C1B7458AC77976EC788E4439C
SHA-512:	E40F27C1D30E5AB4B3DB47C3B2373381489D50147C9623D853E5B299364FD65998F46E8E73B1E566FD79E97AA7B20354CD3C8C79F15372C147FED9C913FFB10
Malicious:	false
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\font-awesome[1].css	
Preview:	/*!. * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */./* FONT PATH. * -------------------------- */.@font-face {. font-family: 'FontAwesome';. src: url('../fonts/fontawesome-webfont.eot?v=4.7.0');. src: url('../fonts/fontawesome-webfont.eot?#iefix&v=4.7.0') format('embedded-opentype'), url('../fonts/fontawesome-webfont.woff2?v=4.7.0') format('woff2'), url('../fonts/fontawesome-webfont.woff?v=4.7.0') format('woff'), url('../fonts/fontawesome-webfont.ttf?v=4.7.0') format('truetype'), url('../fonts/fontawesome-webfont.svg?v=4.7.0#fontawesomeregular') format('svg');. font-weight: normal;. font-style: normal;.}..fa {. display: inline-block;. font: normal normal normal 14px/1 FontAwesome;. font-size: inherit;. text-rendering: auto;. -webkit-font-smoothing: antialiased;. -moz-osx-font-smoothing: grayscale;.}./* makes the font 33% larger relative to the icon container */..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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):	20495
Entropy (8bit):	5.217693761954058
Encrypted:	false
SSDEEP:	384:f5LFrVVVnCQvIR/CFU4hHPV4kdxXvYqo2D75zCx+vI2am3MxGpGTgd/9jt9+Db9A:hNVVVnyiU41xXvlD7wx+v0xyGTgnZO9A
MD5:	6B08DDC901000D51FA1F06A35518F302
SHA1:	BAFE987C18CBE0587DE3E6360E7DA40A2885614B
SHA-256:	02835066969199E9924F1332F7172A5D7E552F023A20C3D8BA03BB6C51CE5BE5
SHA-512:	7A97FA1CF4A12D0F338090F8A4FFAD48D91843D6955304DE5F6208DE394642B0B412D6FD30D7A880CAD92200A8F7F2005C40324BCCE3CFEDA7B14A57DFF098(A
Malicious:	false
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.0/umd/popper.min.js
Preview:	/*. Copyright (C) Federico Zivolo 2018. 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|overlay)/.test(r+s+p)?e:n(o(e))}function r(e){if(!e)return document.documentElement;for(var o=ie(10)?document.body:null,n=e.offsetParent;n===o&&e.nextElementSibling;)n=(e=e.nextElementSibling).offsetParent;var i=n&&n.nodeName;return i&&'BODY'!==i&&'HTM

C:\Users\user\AppData\Local\Temp\~DF21DEBDFF8AE13ED9.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4814023687122488
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loHF9loF9lW8+/GRpKB:kBqoIOw8+/GRe
MD5:	211576761FCBDC9F817576369748FEDE
SHA1:	73DF5B92C1C3089D8F6155DCF1C70FB7E3404F5F
SHA-256:	5A1025D99BDFA3BFEEA11DE3EDBAD988B073B2A9A9F331D3AB0BE6C922F65244
SHA-512:	4149C9653A19BB1ABC5346872F13A8C23E8BA1086FD5F3F4C437EC0A5DD3505E825983C21A11A74CEA36535B963572345844459BA014E3B94B0D3C613EB6DEFB
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF3DB5A53056DE5405.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	36343
Entropy (8bit):	0.6467613763839257
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+lLpYUIU3CasEock6O9CIrock6O9c6s26sF6sy0yc:kBqoxKAuvScS+lLpY7Mse
MD5:	7085EA4DFB5ABB20D619EF4E95C0FEA5
SHA1:	DF5E44A3B915DEAFA18DE057D3A7FC177A4F4799
SHA-256:	9EC090219B43821FA8C18A6AC11C9F702B1B479249A8B1A1C8F8EA808DB85466
SHA-512:	277FDAE86026211F04649969E7E0F63D7357CC39808CDB56EAC5C3031B68FE2364801E15DA7BC731E68BC3EFE604D2DC6016BE8B2BFA46669B029DDC63AF17
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF973A53439F94DBC8.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.43596449973681184
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAi:kBqoxxJhHWSVSEab
MD5:	DF53CE7F414EB2F1EB816346743A73AD
SHA1:	57B0A7449C3F5CC51A0A86A61A958D492DC15940
SHA-256:	20385844397E8C91E91ED89753894ED6ACEB3E0BF55265089C770492EFCBFE6F
SHA-512:	5376E222E2606EE4174B005CF1366D98DAA64D454EAFA73ED3ECF953D784D648284B0B719EFB140C01D2C43B8FFE55F6619D12DB7C232F8C0275813CEF4937A
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

General	
File type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Entropy (8bit):	6.0452559677446756
TrID:	
File name:	One Note shergott@vivaldicap.com.html
File size:	438425
MD5:	6b9c5e9bfcf2518f66e80e941257ad09
SHA1:	85c854dfc0e3ef1a85aaeb17d7a2b5ccd5b8dbaa
SHA256:	ffb4ba9437ffe8c45168b3ab63006d1c7a2e38815f6da1ca37875c5855b6f5e9
SHA512:	bfd7554331e04c0943340e961ee932f892a72faac3c9a598a93be5bfdff2e3b42e7fa83f35bdbeae88e995e6d0fac046d88354e943b308f84a90948346c251c0
SSDEEP:	12288:VGDKhf2yW1MBoU2DY77S4C6Nu1xlvm2JfMDqB:GKhfvWAl/SOup6Mi
File Content Preview:	....<html dir="ltr" class="" lang="en">....<head>.. <title>Sign in to your account</title>.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <meta http-equiv="X-UA-Compatible" content="IE=edge">.. <meta name="viewport" co

File Icon

Icon Hash:	f8c89c9a9a998cb8

Network Behavior

Network Port Distribution

Total Packets: 93

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:24:04.521193981 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.522303104 CET	49719	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.565865040 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.565999985 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.566914082 CET	443	49719	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.566988945 CET	49719	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.583189011 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.586226940 CET	49719	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.630162954 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.630925894 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.630949020 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.631027937 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.633471012 CET	443	49719	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.634536982 CET	443	49719	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.634561062 CET	443	49719	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.634593010 CET	49719	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.634614944 CET	49719	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.672527075 CET	49719	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.673715115 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.684494972 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.684926987 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.685076952 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.685627937 CET	49719	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.717247009 CET	443	49719	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.717473030 CET	443	49719	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.717535019 CET	49719	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.717585087 CET	443	49719	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.717626095 CET	49719	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.718271017 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.718343973 CET	49719	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.720487118 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.720509052 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.720541000 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.720571041 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.721256971 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.729290962 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.729338884 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.729502916 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.730165958 CET	443	49719	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.731249094 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.731329918 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.732039928 CET	443	49719	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.732131004 CET	49719	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.740653038 CET	443	49718	104.16.18.94	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:24:04.740672112 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.740688086 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.740703106 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.740720034 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.740735054 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.740736961 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.740760088 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.740802050 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.741568089 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.741588116 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.741641045 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.741695881 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.742791891 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.742814064 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.742866993 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.742889881 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.743611097 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.743628025 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.743678093 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.744827986 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.744852066 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.744880915 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.744900942 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:04.809899092 CET	443	49719	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.811299086 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:04.970282078 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:05.015263081 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:05.034324884 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:05.034347057 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:05.034394026 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:05.034419060 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:05.034478903 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:05.034497023 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:05.034521103 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:05.034554005 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:05.035564899 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:05.035597086 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:05.035614967 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:05.035635948 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:05.036598921 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:05.036629915 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:05.036664963 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:05.036684036 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:05.037727118 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:05.037753105 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:05.037791967 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:05.037816048 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:05.038707018 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:05.038727045 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:05.038764954 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:05.038790941 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:05.039768934 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:05.039833069 CET	443	49718	104.16.18.94	192.168.2.3
Feb 22, 2021 20:24:05.039844036 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:05.039868116 CET	49718	443	192.168.2.3	104.16.18.94
Feb 22, 2021 20:24:05.040836096 CET	443	49718	104.16.18.94	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:23:53.917119026 CET	51281	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:23:53.968430996 CET	53	51281	8.8.8.8	192.168.2.3
Feb 22, 2021 20:23:54.026047945 CET	49199	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:23:54.077351093 CET	53	49199	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:23:54.909595013 CET	50620	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:23:54.958465099 CET	53	50620	8.8.8.8	192.168.2.3
Feb 22, 2021 20:23:56.106601954 CET	64938	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:23:56.158128977 CET	53	64938	8.8.8.8	192.168.2.3
Feb 22, 2021 20:23:57.254170895 CET	60152	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:23:57.305696011 CET	53	60152	8.8.8.8	192.168.2.3
Feb 22, 2021 20:23:58.197112083 CET	57544	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:23:58.247150898 CET	53	57544	8.8.8.8	192.168.2.3
Feb 22, 2021 20:23:58.269953012 CET	55984	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:23:58.331357956 CET	53	55984	8.8.8.8	192.168.2.3
Feb 22, 2021 20:23:59.193259954 CET	64185	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:23:59.243853092 CET	53	64185	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:00.364048004 CET	65110	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:00.418037891 CET	53	65110	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:01.587955952 CET	58361	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:01.645214081 CET	53	58361	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:02.869903088 CET	63492	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:02.918737888 CET	53	63492	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:03.246488094 CET	60831	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:03.305141926 CET	53	60831	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:04.454263926 CET	60100	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:04.456882954 CET	53195	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:04.458137989 CET	50141	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:04.504514933 CET	53	60100	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:04.507059097 CET	53	53195	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:04.516799927 CET	53	50141	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:04.533310890 CET	53023	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:04.546659946 CET	49563	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:04.581965923 CET	53	53023	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:04.598110914 CET	53	49563	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:06.088310003 CET	51352	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:06.139827013 CET	53	51352	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:07.066112041 CET	59349	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:07.114753008 CET	53	59349	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:08.045578957 CET	57084	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:08.094221115 CET	53	57084	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:08.987473965 CET	58823	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:09.036174059 CET	53	58823	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:09.993308067 CET	57568	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:10.052656889 CET	53	57568	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:11.506706953 CET	50540	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:11.555341959 CET	53	50540	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:12.772020102 CET	54366	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:12.820681095 CET	53	54366	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:13.887051105 CET	53034	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:13.944127083 CET	53	53034	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:30.007122993 CET	57762	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:30.068345070 CET	53	57762	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:33.257446051 CET	55435	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:33.306993961 CET	53	55435	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:34.053026915 CET	50713	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:34.107783079 CET	53	50713	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:34.270385027 CET	55435	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:34.318974972 CET	53	55435	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:35.069353104 CET	50713	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:35.120852947 CET	53	50713	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:35.271265984 CET	55435	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:35.320141077 CET	53	55435	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:36.085877895 CET	50713	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:36.137348890 CET	53	50713	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:37.270709991 CET	55435	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:37.319323063 CET	53	55435	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:38.124228001 CET	50713	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:38.177973986 CET	53	50713	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:24:41.286703110 CET	55435	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:41.337729931 CET	53	55435	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:42.119637966 CET	50713	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:42.171150923 CET	53	50713	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:46.365731955 CET	56132	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:46.421334982 CET	53	56132	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:49.560808897 CET	58987	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:50.590615988 CET	58987	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:51.251800060 CET	56579	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:24:51.294336081 CET	53	58987	8.8.8.8	192.168.2.3
Feb 22, 2021 20:24:51.303329945 CET	53	56579	8.8.8.8	192.168.2.3
Feb 22, 2021 20:25:16.790894032 CET	60633	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:25:16.852385998 CET	53	60633	8.8.8.8	192.168.2.3
Feb 22, 2021 20:25:38.932782888 CET	61292	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:25:38.991930962 CET	53	61292	8.8.8.8	192.168.2.3
Feb 22, 2021 20:25:46.568265915 CET	63619	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:25:46.640692949 CET	53	63619	8.8.8.8	192.168.2.3
Feb 22, 2021 20:26:00.232171059 CET	64938	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:26:00.285854101 CET	53	64938	8.8.8.8	192.168.2.3
Feb 22, 2021 20:26:00.806335926 CET	61946	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:26:00.863430023 CET	53	61946	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 20:24:04.454263926 CET	192.168.2.3	8.8.8.8	0x1a59	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Feb 22, 2021 20:24:04.456882954 CET	192.168.2.3	8.8.8.8	0x3b00	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Feb 22, 2021 20:24:04.533310890 CET	192.168.2.3	8.8.8.8	0x3f64	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)
Feb 22, 2021 20:24:04.546659946 CET	192.168.2.3	8.8.8.8	0x149a	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 20:24:04.504514933 CET	8.8.8.8	192.168.2.3	0x1a59	No error (0)	maxcdn.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 20:24:04.507059097 CET	8.8.8.8	192.168.2.3	0x3b00	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Feb 22, 2021 20:24:04.507059097 CET	8.8.8.8	192.168.2.3	0x3b00	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Feb 22, 2021 20:24:04.581965923 CET	8.8.8.8	192.168.2.3	0x3f64	No error (0)	stackpath.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 20:24:04.598110914 CET	8.8.8.8	192.168.2.3	0x149a	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 22, 2021 20:24:04.630949020 CET	104.16.18.94	443	192.168.2.3	49718	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Feb 22, 2021 20:24:04.634561062 CET	104.16.18.94	443	192.168.2.3	49719	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6148 Parent PID: 792

General

Start time:	20:24:03
Start date:	22/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7117d0000
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: 6200 Parent PID: 6148

General

Start time:	20:24:03
Start date:	22/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6148 CREDAT:17410 /prefetch:2
Imagebase:	0x3c0000
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