ID: 283702
Cookbook: browseurl.jbs
Time: 00:31:33
Date: 10/09/2020
Version: 29.0.0 Ocean Jasper

Table of Contents

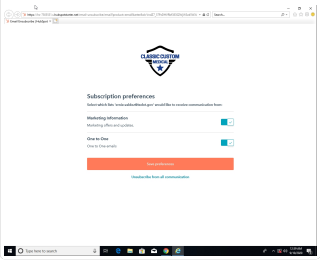
Analysis Report https://hs-7505531.s.hubspotstarter.net…

Overview

General Information

Sample URL:	http://https://hs-7505531.s.hubspotstarter.net/email-unsubscribe/email?product=emailStarter&d=VndZ7_57PzDHVRbf383SZtVjW3zd5WX4tcv12W3H91db3P4GWRW7_Nbz01fk4d_Vky9Mm5GrNXlW5HScjd62JJjxW6PpYRM2R6jc5N5B5t5nGKd_PV20N5J40Pn0TW8-NgKB5sJr80F6ckDhDJX0h1&v=2&email=ernie.valdez%40txdot.gov&utm_source=hs_email&utm_medium=email&utm_content=94880919&_hsenc=p2ANqtz-_t-qGyKf9L54VQYC06zkNpDt2b-DzT7t21bDE0behJn7nwzoe_XYr4aUmR4iWxXFG_bOWi31g3m_VRpgKaEsTuR5573w&_hsmi=94880919
Analysis ID:	283702

Most interesting Screenshot:



Detection

Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification

Startup

- **System is w10x64**
- iexplore.exe (PID: 6664 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6716 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6664 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

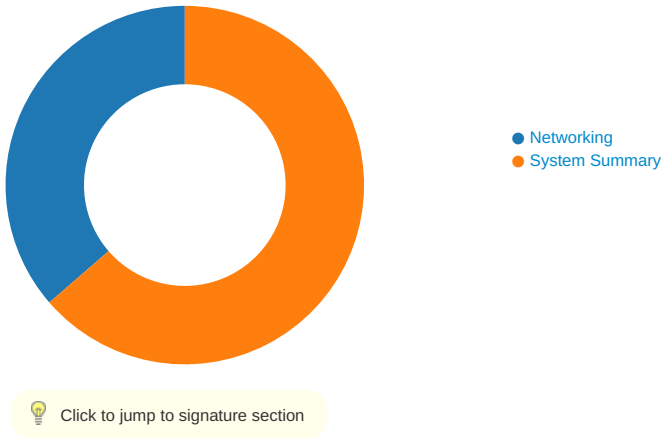
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

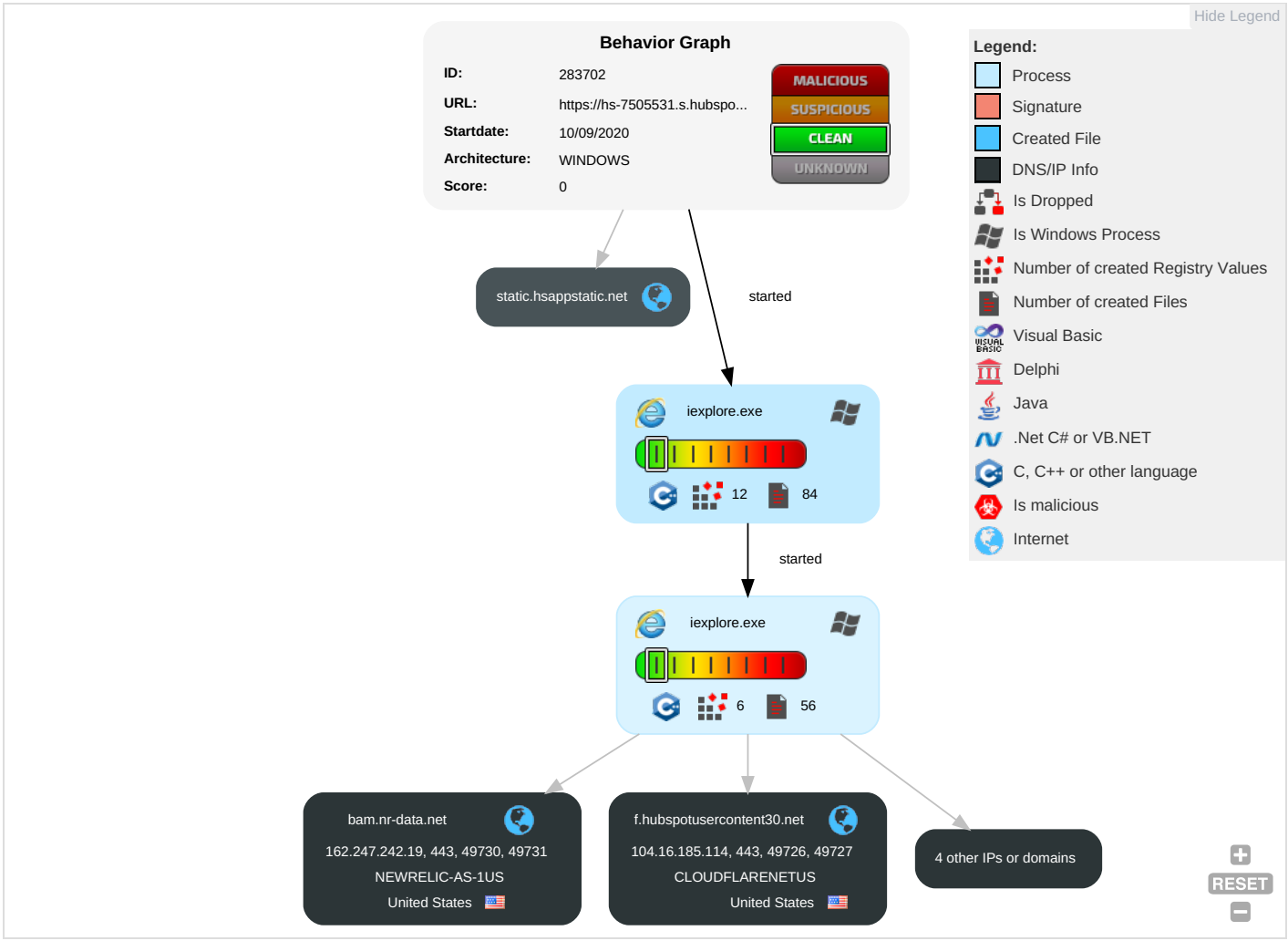


There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

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

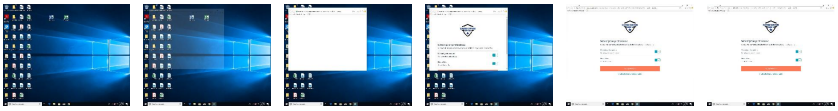
Behavior Graph

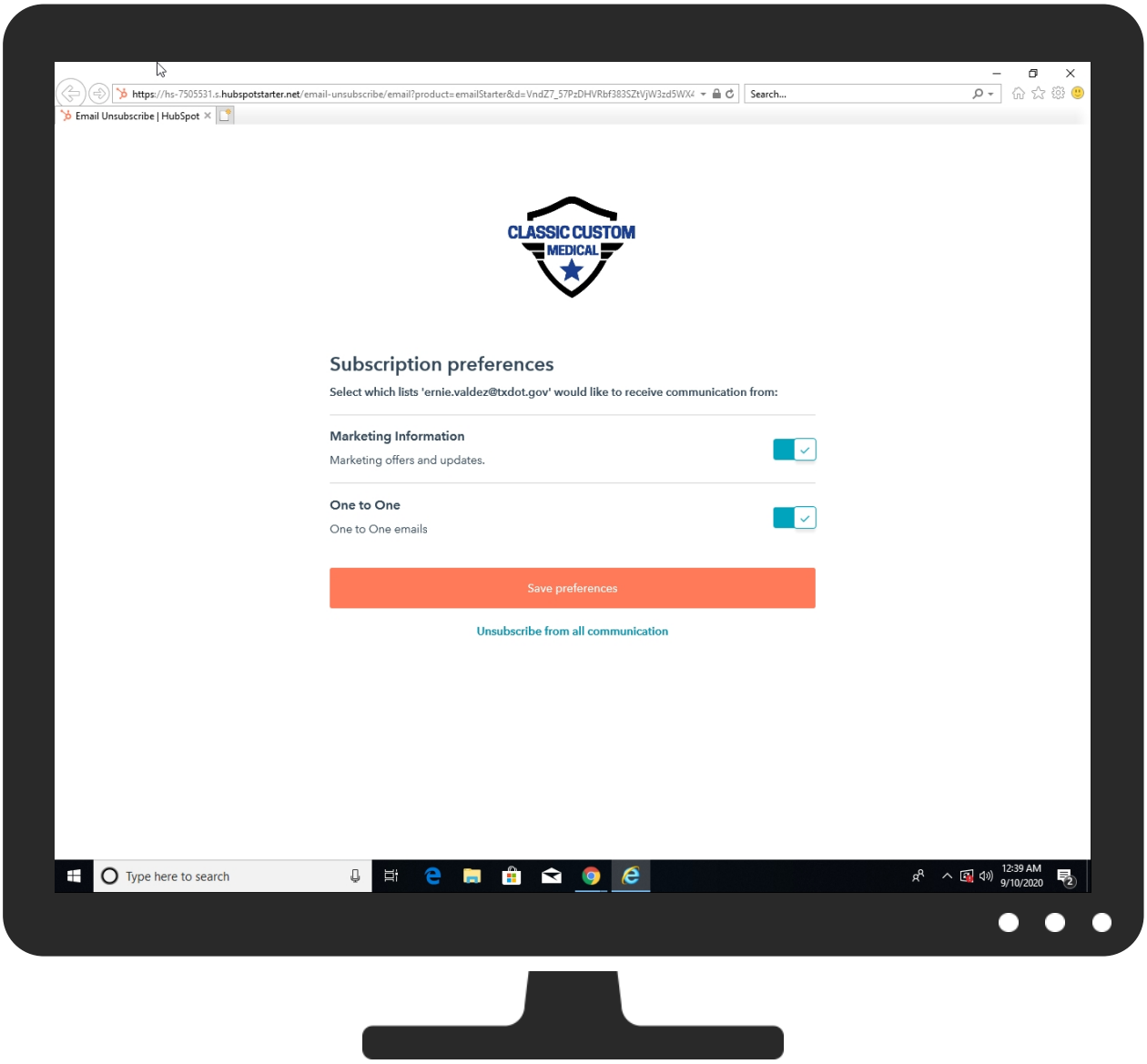


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://hs-7505531.s.hubspotstarter.net/email-unsubscribe/email?product=emailStarter&d=VndZ7_57PzDHVRbf383SZtVjW3zd5WX4tcv12W3H91db3P4GWRW7_Nbz01fk4d_Vky9Mm5GrNXlW5HScjd62JJjxW6PpYRM2R6jc5N5B5t5nGKd_PV20N5J40Pn0TW8-NgKB5sJr80F6ckDhDJX0h1&v=2&email=ernie.valdez%40txdot.gov&utm_source=hs_email&utm_medium=email&utm_content=94880919&_hsenc=p2ANqtz-_t-qGyKf9L54VQYC06zkNpDt2b-DzT7t21bDE0behJn7nwzoe_XYr4aUmR4iWxXFG_bOWi31g3m_VRpgKaEsTuR5573w&_hsmi=94880919	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
static.hsappstatic.net	0%	Virustotal		Browse
bam.nr-data.net	0%	Virustotal		Browse
f.hubspotusercontent30.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Medium.woff2)	0%	Avira URL Cloud	safe	
http://https://api.hubspot	0%	Avira URL Cloud	safe	
http://https://static.hsappstatic.net/StyleGuideUI/static-3.205/img/sprocket/favicon-32x32.png	0%	Avira URL Cloud	safe	
http://https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Demi.woff2)	0%	Avira URL Cloud	safe	
http://https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Regular.woff2)	0%	Avira URL Cloud	safe	
http://https://static.hsappstatic.net	0%	Virustotal		Browse
http://https://static.hsappstatic.net	0%	Avira URL Cloud	safe	
http://https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Bold.woff2)	0%	Avira URL Cloud	safe	
http://https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Regular.woff)	0%	Avira URL Cloud	safe	
http://www.wikipedia.com/	0%	Virustotal		Browse
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://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Medium.woff)	0%	Avira URL Cloud	safe	
http://https://hs-7505531.s.hubspotstarter.net/email-unsubscribe/email?product=emailStarter&d=VndZ7_57PzDHV	0%	Avira URL Cloud	safe	
http://https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Bold.woff)	0%	Avira URL Cloud	safe	
http://https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Demi.woff)	0%	Avira URL Cloud	safe	
http://https://f.hubspotusercontent30.net/hubfs/7505531/MEDICAL%20(3).png	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
static.hsappstatic.net	104.17.5.210	true	false	• 0%, Virustotal, Browse	unknown
api.hubspot.com	104.19.154.83	true	false		high
bam.nr-data.net	162.247.242.19	true	false	• 0%, Virustotal, Browse	unknown
hs-7505531.s.hubspotstarter.net	104.17.123.201	true	false		unknown
f.hubspotusercontent30.net	104.16.185.114	true	false	• 0%, Virustotal, Browse	unknown
js-agent.newrelic.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.nytimes.com/	msapplication.xml4.1.dr	false		high
http://https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Medium.woff2)	project[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://api.hubspot	custom-quick-fetch[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://static.hsappstatic.net/StyleGuideUI/static-3.205/img/sprocket/favicon-32x32.png	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Demi.woff2)	project[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.youtube.com/	msapplication.xml8.1.dr	false		high
http://https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Regular.woff2)	project[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://static.hsappstatic.net	email[1].htm.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Bold.woff2)	project[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Regular.woff)	project[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.wikipedia.com/	msapplication.xml7.1.dr	false	• 0%, Virustotal, Browse • 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.xml3.1.dr	false		high
http://https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Medium.woff)	project[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.reddit.com/	msapplication.xml5.1.dr	false		high
http://www.twitter.com/	msapplication.xml6.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://hs-7505531.s.hubspotstarter.net/email-unsubscribe/email?product=emailStarter&d=VndZ7_57PzDHV	{AFEE1507-F338-11EA-90E8-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Bold.woff)	project[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Demi.woff)	project[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://f.hubspotusercontent30.net/hubfs/7505531/MEDICAL%20(3).png	portal-information[1].json.2.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Country	Flag	ASN	ASN Name	Malicious
104.17.5.210	United States		13335	CLOUDFLARENETUS	false
104.19.154.83	United States		13335	CLOUDFLARENETUS	false
104.16.185.114	United States		13335	CLOUDFLARENETUS	false
162.247.242.19	United States		23467	NEWRELIC-AS-1US	false
104.17.123.201	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	29.0.0 Ocean Jasper
Analysis ID:	283702
Start date:	10.09.2020
Start time:	00:31:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs

Sample URL:	http://https://hs-7505531.s.hubspotstarter.net/email-unsubscribe/email?product=emailStarter&d=VndZ7_57PzDHVRbf383SZtVjW3zd5WX4tcv12W3H91db3P4GWRW7_Nbz01fk4d_Vky9Mm5GrNXlW5HScjd62JJjxW6PpYRM2R6jc5N5B5t5nGKd_PV20N5J40Pn0TW8-NgKB5sJr80F6ckDhDJX0h1&v=2&email=ernie.valdez%40txdot.gov&utm_source=hs_email&utm_medium=email&utm_content=94880919&_hsenc=p2ANqtz-_t-qGyKf9L54VQYC06zkNpDt2b-DzT7t21bDE0behJn7nwzoe_XYr4aUmR4iWxXFG_bOWi31g3m_VRpgKaEsTuR5573w&_hsmi=94880919
Analysis system description:	w10x64 Windows 10 64 bit v1803 with Office Professional Plus 2016, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@3/38@7/5
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.158.208.111, 51.143.111.7, 104.83.120.32, 151.101.2.110, 151.101.66.110, 151.101.130.110, 151.101.194.110, 51.104.139.180, 23.10.249.26, 23.10.249.43, 23.54.113.104, 152.199.19.161, 93.184.221.240, 52.155.217.156, 52.164.221.179 • Excluded domains from analysis (whitelisted): umwatson.trafficmanager.net, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, wu.azureedge.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, ie9comview.vo.msecnd.net, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, f4.shared.global.fastly.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, go.microsoft.com.edgekey.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\OWKXBYV9\hs-7505531.s.hubspotstarter[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Size (bytes):	26
Entropy (8bit):	2.469670487371862
Encrypted:	false
MD5:	132294CA22370B52822C17DCB5BE3AF6
SHA1:	DD26B82638AD38AD471F7621A9EB79FED448A71C
SHA-256:	451ABBE0AEFC000F49967DABF8D42344D146429F03C8C8D4AE5E33FF9963CF77
SHA-512:	6D5808CAD199A785C82763C68F0AE1F4938C304B46B70529EA26B3D300EF9430AD496C688D95D01588576B3A577001D62245D98137FD5CD825AD62E17D36F15C
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{AFEE1505-F338-11EA-90E8-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Size (bytes):	30296
Entropy (8bit):	1.848314994401748
Encrypted:	false
MD5:	4564C8582F93CAB73BF7FC1C9718B279
SHA1:	E8E883FBCBD3CB0D6818F4466C93F22081F36912
SHA-256:	532F767FAF20A6EBE5071DC37F8F47FE51646331CF8A0EE7376C6C544526C277
SHA-512:	31ED37FF0276C2ACC215E60F84CEC5A98549E215D84112919E32B20B3CB12659D0B7AA094C1D4EC9D8B97C95D572A4485C77F97CF84A63EE6C69176D091D55E
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\{AFEE1507-F338-11EA-90E8-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{AFEE1507-F338-11EA-90E8-ECF4BBEA1588}.dat	
File Type:	Microsoft Word Document
Size (bytes):	32276
Entropy (8bit):	2.4425534955425645
Encrypted:	false
MD5:	49B8150D5A137B9F2E3B35EC9094672E
SHA1:	A791A04A6EB709A69B89928C88239D44EACBE529
SHA-256:	65801A488D264CDC87457DD9090FFA17FAABDCE3FC978759C7DCBB703D437655
SHA-512:	5A1286212B8F04A51A1755D418A37DD3FF654B88CDC80C3F1A2C8F06BB003C1989B8EDBF61762721110FD9DC173B7C590D1C3144D7D4C180A7073E1638B10FA
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\{B6534829-F338-11EA-90E8-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Size (bytes):	16984
Entropy (8bit):	1.5644817382385656
Encrypted:	false
MD5:	5503A737C079A68E7826FDC1026628B9
SHA1:	7B69A936B91B010CB5B60740597D77CACB8CA842
SHA-256:	F01C21D006DD4DEF152D4D99A7733429F81E4561B7F73242343D9982D2F12076
SHA-512:	9246E1A51F5978782FE3D210D75FE67B7AB14B492E435C003B99DF23A1A73423236C308794F77A059057A4EF1A71055358CFE740BB24A41723650C50C88A584C
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
Size (bytes):	656
Entropy (8bit):	5.102126036612407
Encrypted:	false
MD5:	F627530F34C1EE48BFE0B690C4A4BF72
SHA1:	A0E5B977C878907A6CAC4AAA99E94565E309994A
SHA-256:	7394CC6DD82CD3E16794C5DAF2DF19F3752B2941F6B0E79DFC854EF1C762ED12
SHA-512:	7119A47541960468959CC308219D5CA235F24031F74AD8396F4FB9F3B37AA870E0E0AEF94FEF72943266C93EA3E53977E32D671B9CC019129F6D0B3E5372B379
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x874aaa4b,0x01d68745</date><accdate>0x874aaa4b,0x01d68745</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>0x874aaa4b,0x01d68745</date><accdate>0x874aaa4b,0x01d68745</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
Size (bytes):	653
Entropy (8bit):	5.145723881632606
Encrypted:	false
MD5:	B1C8F17FDEFFBF689339947A81DDA036
SHA1:	4080FBDA2B234BE544E19A25BA06BB6CC644AED0
SHA-256:	3007B1395C25CF0650D9F4DB33C24F8DA4D43D1D1FF07392160B0DAF925E3BC6
SHA-512:	F13E935670CD75DE95ADC164BB3AAA573FBD19B1EE1E213CAFDAAF350B19D2C689678D8EB8894B07113A954B0F5336084F55D33DDA326758F080D406A9DE43E
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>0x87412110,0x01d68745</date><accdate>0x87412110,0x01d68745</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>0x87412110,0x01d68745</date><accdate>0x87412110,0x01d68745</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
Size (bytes):	662
Entropy (8bit):	5.120004144214406
Encrypted:	false
MD5:	54A41CC847F77C80807D26A7F1DF3682
SHA1:	59CAB8258B394B62D6115033353FB129FCB2607B
SHA-256:	5CDAD6122AF246701C398C84BB4C6F6BF3211B989AB766F88FD15C72F14C1A1C
SHA-512:	072EC01C78E17DD284B61A4AF734F7ABC2B829541588A6FCDBDC3FF078C152AE65519BB1A6A6657C93C2C6E17AFF1C20849B7A2FC751514C95F762A02BBAE7 9
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x874aaa4b,0x01d68745</date><accdate>0x874aaa4b,0x01d68745</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>0x874aaa4b,0x01d68745</date><accdate>0x874aaa4b,0x01d68745</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-314712940\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
Size (bytes):	410
Entropy (8bit):	5.188828259346642
Encrypted:	false
MD5:	A5D5618D9ED59B27D70396B4D24521C8
SHA1:	1285B10A7F36AC06153DF2AD11B3C760A8F6C5D9
SHA-256:	7E6507DD2F8CEAE6C25A939B8E459DF2F68FBDC3135A619F97D0FDD3129F515E
SHA-512:	A7BAC94A187FD71F9FAF03177C2725E037464FB845ADFA7CF9D5F318621863F9E4386DC2AC5774025AD3FC7DC75FABC6830C87687EB7E6DAFD2A723620AD45 A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://go.microsoft.com/fwlink/p/?LinkId=255142"/><date>0x259f0d0f,0x01d52d14</date><accdate>0x87438326,0x01d68745</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Bing.url"/><selection>\lowres.png</selection></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
Size (bytes):	647
Entropy (8bit):	5.125415033199938
Encrypted:	false
MD5:	BE54EB3980E493020F1039DBC1D14A17
SHA1:	D8703AABE91B273AD78B37EAFB540FE839C7CC3F
SHA-256:	C8A035DFAF5246D610E5F29E2A858C3479D9C8FCD723EEE37FE316BF35F18D62
SHA-512:	3E0E724B269987872C956F05A8B48BA5C76A79960926A7F97E9025605DFFD016FDECBF111C2E578F7244AFEFECC7C245C1416A3E9FEAC2D9DFCB3F0647B237C 5
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x874847ef,0x01d68745</date><accdate>0x874847ef,0x01d68745</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>0x874847ef,0x01d68745</date><accdate>0x874847ef,0x01d68745</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
Size (bytes):	656
Entropy (8bit):	5.148617816865642

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Encrypted:	false
MD5:	80A92C21A90CBC3C337218F6819E71B2
SHA1:	D1AA79D5E11231337DB9FD1AC5FF2D2A319AC460
SHA-256:	DEC38363E168FF6EEE71E97FBE1B242652FDA4BD0367D679F363E44FDB1A4B1F
SHA-512:	AA075E72348C24950AA47E48D5EBCCD6A251A3D4A267B896E34CA256AB4AA1BEEC5FA2A3FDD624660CEEAF525DD36842CAFB9C5CF5556C6EFEA6A938B2D8 FDF
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x874d0c9d,0x01d68745</date> accdate>0x874d0c9d,0x01d68745</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>0x874d0c9d,0x01d68745</date><accdate>0 x874d0c9d,0x01d68745</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
Size (bytes):	653
Entropy (8bit):	5.113568008333224
Encrypted:	false
MD5:	715A430A1FBE1D90FF8DB59386A16D78
SHA1:	A1CF8D543CD0D8EB99E50CCA45EE6DED826D901C
SHA-256:	BB5EC0569F7CE851238D77F742AFDF9FC676EA4D39AAC8F08F95CC0BE348E022
SHA-512:	62985D09A0F9B7BC569AF69251AF418CD87A781F89B869F9A79FF728831DF0CC53FEDD2176C3D7627FB10B3C35E02CFB3EE046EB5C845DCFC648851C7AA560 B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x874847ef,0x01d68745</date><a ccdate>0x874847ef,0x01d68745</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>0x874847ef,0x01d68745</date><accdate>0x8 74847ef,0x01d68745</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
Size (bytes):	656
Entropy (8bit):	5.149368454379586
Encrypted:	false
MD5:	A65818992CE3A4FC2E3BB9C5D73498C4
SHA1:	7A4205E93233D695D233C6174C628E0FDD9C2C5D
SHA-256:	4E7433E5EA46E0811FEC78C38ABA927461FD73DB586DC5B78772A803FD55CF44
SHA-512:	2CCE10F383A6043DBB14A119FD71C19BFCFD4FD0BF6FF6F0936187D81655A436F484883738D5AE95AD05AEB3DC42D21D3D385B847D9170807E3DB8B5A2FFBF A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x874847ef,0x01d68745</date> accdate>0x874847ef,0x01d68745</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>0x874847ef,0x01d68745</date><accdate>0 x874847ef,0x01d68745</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
Size (bytes):	659
Entropy (8bit):	5.154913890422455
Encrypted:	false
MD5:	34E4578799C22AEF64136ED6DD116B82
SHA1:	03DA3E1018D7A068A94A7D026A899DDE08445701
SHA-256:	A59FAFBC9B826E9FF27BBFD5618412CD92CE5E1022A91959D93C6C50A427251C
SHA-512:	5097E0A71DC320D595ECE477B318705C3C7D5F4E6BDFD09C8FF0773C4E32E5D751A5FA211A13B8C76B7B90C942ADF9C09B7B1B27F72C105660A2DC84E3B03E B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x8745e594,0x01d68745</date> <accdate>0x8745e594,0x01d68745</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>0x8745e594,0x01d68745</date><accdate >0x8745e594,0x01d68745</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
Size (bytes):	653
Entropy (8bit):	5.134838520976002
Encrypted:	false
MD5:	4FE079ED84915E1D45416C18D0F4A9D5
SHA1:	092CD2A897345089F2045ED1E41DACAACA8E877B
SHA-256:	DBCED181C0026E295C75967548F094C9075D3FB39FD0C107159B446D2451E58C
SHA-512:	D31A9486ADDDC37B9FD0C8EE8721C6A00B3B02C7DE010D9E28DFCD12AFA7E4E15871F7853D6A30ED1DBE0D03B681D02A2FF9FB0B39EABD39EDF674BEE196 443
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x8745e594,0x01d68745</date><a ccdate>0x8745e594,0x01d68745</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>0x8745e594,0x01d68745</date><a ccdate>0x8745e594,0x01d68745</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Go ogle.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Size (bytes):	1369
Entropy (8bit):	6.169352748634554
Encrypted:	false
MD5:	1A7576B3F8338EA286D6F59CB89CFDD9
SHA1:	3659FECD162A269448E20EB400FB3BC048FF84D6
SHA-256:	F398E934AC558EE514D3FF544E6F835347B1FDB35B6EFA0A9CDFEEB22C932A80
SHA-512:	63D6EE020DEED8E459890E8FD4B475D0C5E79092ACE2B27EA7DDDF707850C8156B5456A98C2A991D4298D36B68EFAFA94F0059B288FAF61C70D0E0F016D346 0
Malicious:	false
Reputation:	low
Preview:	W.h.t.t.p.s.:././.s.t.a.t.i.c...h.s.a.p.p.s.t.a.t.i.c...n.e.t./.S.t.y.l.e.G.u.i.d.e.U.I./.s.t.a.t.i.c.-.3...2.0.5./.i.m.g./.s.p.r.o.c.k.e.t./.f.a.v.i.c.o.n.-.3.2.x.3.2...p.n.g......PNG........IHDR... ... .D.......gAMA......a.... cHRM..z&.............u0...`..:....p..Q<....PLTE....zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.z Y.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.z Y.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.z Y.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY...(.......tRNS........'.......s..ER..Yp..,_....`!..Q...N?....z9.....4...d"..X..m..e.......a...&............M.g5.<.[T.f..1..8..6..|...%..IS.y:L..$~.kP....I DAT8...[RA..}.T.....a.1%K...+.)......v.nj...J...n..B,.8_....y.LY...&..%.8u.......Xs..3$.j./...s8.9Q}^..7.3.xH./.\........(...,P.K

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\MEDICAL%20(3)[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 500 x 500, 8-bit/color RGBA, non-interlaced
Size (bytes):	39681
Entropy (8bit):	7.952473490104067
Encrypted:	false
MD5:	C8339C8795A5505E571EB46835264609
SHA1:	902DFEB5C047909C8E25A9486D8C7C5F1B56840E
SHA-256:	786B06BC0F88EA208DFC8E9C84926870D38B275DE01BAD7FF762E8949836E90B
SHA-512:	E86AB64710D008593B14308DD9DC85C6DBCD0240CEF9F15F8E9955EE65F3BB158503079BF032DF1CD5F796A5320EC584365093A92E5AF1F2F4258936FA34F1A9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://f.hubspotusercontent30.net/hubfs/7505531/MEDICAL%20(3).png
Preview:	.PNG........IHDR...................IDATx^..\.G../.nl.).gM41.M.M..k46...K,..M..+..b.]..`.J...i*].+"(..D...@.....5.w..A......\...3...N....A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A. .A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A. .A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A. .A..A..A..A..A..A..A..A..A..A..A.I(...'z..%..Dm..q...Z.5..nh...A..i@8......o.....O.6m.A..]......u.V.C.Jrj...u...O.g.}.:n..}}}........S.?.....t8.. ....u...?...O..=r.GD.8..j.._....>...3...[...&a...x.. .. u.3.m....Z.._.~.eu4.Rt..t........8...;. ..H..k.................k..K..../w.......A..A......._..W.^wd......o...y...!.g.. ..4u..xk__.....+.=...`...S)..c.......{..v.A...A.`{KK...|.A...l..J.....>y..VrM..#.. ..0v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\core[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\core[1].js	
Size (bytes):	33348
Entropy (8bit):	5.296329580888088
Encrypted:	false
MD5:	00EFDCB01D5F747B6C28AF798C84F7CA
SHA1:	3BF2A08184B64D3E80970CEE91F59DE4FF13992A
SHA-256:	5F78A854E2477EB7EBDF6E4CAFD98440B70B789FCDBEE6DDD2B5FB85F3435892
SHA-512:	27931940EE7BB9C3A764ECDE62559008DFD150CF324B0066822DEF470A522F194F4A0E60DF8C6A960F28F34D3ADE0C3475A2CE4CAEC592F2FDBB79B67F81A3 6
Malicious:	false
Reputation:	low
Preview:	!function(){"use strict";function t(t,e){return e={exports:{}},t(e,e.exports),e.exports}var e,n,r,o={}.toString,i=function(t){return o.call(t).slice(8,-1)},u=Array.isArray||function(t){return"Array"==i(t)},a=function(t){return"object"==typeof t?null!==t:"function"==typeof t},c=function(t){if(void 0==t)throw TypeError("Can't call method on "+t);return t},f=function(t){return Object(c(t))},s=Math.ceil,l=Math.floor,p=function(t){return isNaN(t=+t)?0:(t>0?l:s)(t)},v=Math.min,h=function(t){return t>0?v(p(t),9007199254740991):0},d=function(t,e){if(!a(t))return t;var n,r;if(e&&"function"==typeof(n=t.toString)&&!a(r=n.call(t)))return r;if("function"==typeof(n=t.valueOf)&&!a(r=n.call(t)))return r;if(!e&&"function"==typeof(n=t.toString)&&!a(r=n.call(t)))return r;throw TypeError("Can't convert object to primitive value")},g=function(t){try{return!!t()}catch(e){return!0}},y=!g(function(){return 7!=Object.defineProperty({},"a",{get:function(){return 7}}).a}),m="object"==typeof window&&window&&windo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\f9d051f404[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Size (bytes):	24
Entropy (8bit):	2.459147917027245
Encrypted:	false
MD5:	BC32ED98D624ACB4008F986349A20D26
SHA1:	2D3DF8C11D2168CE2C27E0937421D11D85016361
SHA-256:	0C9CF152A0AD00D4F102C93C613C104914BE5517AC8F8E0831727F8BFBE8B300
SHA-512:	71ACC6DA78D5D5BF0EEA30E2EE0AC5C992B00EFEC959077DFE0AB769F1DBBD9AF12D5C5C155046283D5416BEB606A9EF323FB410E903768B1569B69F37075B 4E
Malicious:	false
Reputation:	low
Preview:	GIF89a.....,.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\nr-spa-1169.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Size (bytes):	37554
Entropy (8bit):	5.31517884113122
Encrypted:	false
MD5:	5E3590BFFA49FDDC4BC389E63736DA42
SHA1:	C7F8BDF8337F4F84B1359CB2BD64A2587AEB74AF
SHA-256:	37072A42526245F257B725698D7E70DFAB281BFD00D38F1112DAFD36A6E04176
SHA-512:	A3BF0488CB962945151D66EC3160C58FBA975C85688D0074725B71F09AE79381C718B81AE67F3BACEC493393183222BF24A191042B6962020B4D20B52AFD1818
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://js-agent.newrelic.com/nr-spa-1169.min.js
Preview:	!function(t,n,e){function r(e,o){if(!n[e]){if(!t[e]){var a="function"==typeof __nr_require&&__nr_require;if(!o&&a)return a(e,!0);if(i)return i(e,!0);throw new Error("Cannot find module '"+e+"'")}var s=n[e]={exports:{}};t[e][0].call(s.exports,function(n){var i=t[e][1][n];return r(i||n)},s,s.exports)}return n[e].exports}for(var i="function"==typeof __nr_require&&__nr_require,o=0;o<e.length;o++)r(e[o]);return r}({1:[function(t,n,e){n.exports=function(t,n){return"addEventListener"in window?window.addEventListener(t,n,!1):"attachEvent"in window?window.attachEvent("on"+t,n):void 0}},{}],2:[function(t,n,e){function r(t,n,e,r,o){d[t]||(d[t]={});var a=d[t][n];return a||(a=d[t][n]={params:e||{}},o&&(a.custom=o)),a.metrics=i(r,a.metrics),a}function i(t,n){return n||(n={count:0}),n.count+=1,f(t,function(t,e){n[t]=o(e,n[t])}),n}function o(t,n){return n?(n&&!n.c&&(n={t:n.t,min:n.t,max:n.t,sos:n.t*n.t,c:1}),n.c+=1,n.t+=t,n.sos+=t*t,t>n.max&&(n.max=t),t<n.min&&(n.min=t),n):{t:t}}function a(t,n){return

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\portal-information[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Size (bytes):	206
Entropy (8bit):	5.008042203208693
Encrypted:	false
MD5:	624BC43E77D039CFDE45F5B46BF598D6
SHA1:	BC652F1D9F461A97041FDE7DF34D2CB8BB810552
SHA-256:	94146D5ABCC361D7ECAF77A7D252B4F25EED599E036746D8614D61B90D4C007E
SHA-512:	DB18A08F81AA709EEFF00826B5E2D64C6B10FC3DC885088D3684C6A5EED910F6EDAB24C2A5C3E5BC27D43A97A79A3E9C03248B9AD2F812CBEEB62A8892A64 B73
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\portal-information[1].json	
IE Cache URL:	http://https://api.hubspot.com/subscriptions/v1/preferences/portal-information?d=VndZ7_57PzDHVRbf383SZtVjW3zd5WX4tcv12W3H91db3P4GWRW7_Nbz01fk4d_Vky9Mm5GrNXlW5HScjd62JJjxW6PpYRM2R6jc5N5B5t5nGKd_PV20N5J40Pn0TW8-NgKB5sJr80F6ckDhDJX0h1&product=emailStarter&clienttimeout=15000
Preview:	{"companyName":"Classic Custom Medical","logoUrl":"https://f.hubspotusercontent30.net/hubfs/7505531/MEDICAL%20(3).png","primaryColor":"#388be3","secondaryColor":"","accentColor":"#388be3","accent2Color":""}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\project[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Size (bytes):	1152
Entropy (8bit):	4.9376547871593415
Encrypted:	false
MD5:	8A8B858723C33C4C97CD69BD245D9947
SHA1:	D58FF6F76BAF14A8D8E21CE376E16C5A22B746CD
SHA-256:	429F44281F0ECCB61DF61D41D248E9319A354E6800A594E883785836566929B1
SHA-512:	EEB4F4E06FC8E446A806A3BB3CE228F0EC6831B10F298F4CC708598BC1F9287F1249FCCF8E5155EFF3505F4C05EFB6EDFEDA5B0FF7CDECB309705C6DD13BCD0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.hsappstatic.net/EmailUnsubscribeUI/static-1.3413/bundles/project.css
Preview:	@font-face{font-display:swap;font-family:Avenir Next W02;src:url(https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Regular.woff2) format("woff2"),url(https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Regular.woff) format("woff")}@font-face{font-display:swap;font-family:Avenir Next W02;src:url(https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Medium.woff2) format("woff2"),url(https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Medium.woff) format("woff");font-weight:500}@font-face{font-display:swap;font-family:Avenir Next W02;src:url(https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Demi.woff2) format("woff2"),url(https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Demi.woff) format("woff");font-weight:600}@font-face{font-display:swap;font-family:Avenir Next W02;src:url(https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Bold.woff2) format("woff2"),url(ht

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AvenirNext-Bold[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 33887, version 1.0
Size (bytes):	33887
Entropy (8bit):	7.988829365600527
Encrypted:	false
MD5:	51CDA03B699A5D41430C610EEDB83C58
SHA1:	4200BD7A766EC9DC36205A148CC4E908DAEE1674
SHA-256:	943A5AF8DD4D2C25A74CF054A333B1572B5E30AB507C0933D3684FB95FDA6AB7
SHA-512:	3924904657DB2803D05FFE738ECA6304EC782D236D8FB8C6FE1DE6701485B89E482C3C77CDF940516D327BC5723FD4AED268F7E2B768AF49612966EA94032588
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Bold.woff
Preview:	wOFF....._.....*h.....}x.....v.....GPOS...l.....#...OS/2.....V...`g...VDMX...T.....o.w5cmap.....t....cvt .....Z.....~.hfpgm...D...+...P...gasp...p.....glyf...x..V.....>..)head..lP…6...6....hhea..l....!...$....hmtx..l.....O.2.loca..o.....Dmaxp..sp... ... .name..s.....post..{..... ...2prep..{...../..[.x..yl\W..c.=^f.xK...6^..%.,n....mH...)$-H@KT...@.....UT..h.b.....*(e1.....P....P....%Bz|..7..=.Olg.>...w.=..s~..gC..p..C>..... ...n.BS..*....W.....o....m.e.<g..9g8.L..9g!..w.s7.4o.<.y....9m3inZ..9.}..6.q...i.".}...b.. ..C.a..1|.O.x...EL0.....F=..F....l.Fl.v..^.!;._.dP.d..q.5.;.Q..4.4...g;....5.....D...{9l.d...{.[p.f.&x.m.....6...^....(.6#,,.?..OX..i..kaS.N.rz.P..9.5i.[..)FJ:m.Yghu,.6'8.....K..k.J..6...5..01.9...v.....N.&..1...W..!.p-...9Nz.w.i.;.r.%q1t!=1d.\..8..js.d].[...l'.Ssk.hm..._..a.O....2W.iv..m+A....U.zUkND.....-.F\.....[.f>o..|.z.....:..B..w...r.:^...2...I.6c.5J^.^.`=nFf=a{.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AvenirNext-Demi[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 33514, version 1.0
Size (bytes):	33514
Entropy (8bit):	7.987272876955452
Encrypted:	false
MD5:	2C70E1E58EC4E3ED9B7364BBDA5C1F80
SHA1:	CBA048D0C8DD1A2F9D2338B3D9C1AE04EA15353C
SHA-256:	CA7992D13F81B8BE9B981157E13C4E70FFC2AB5FA6B03B01C7EDD47902E1AE73
SHA-512:	D879B13414C5149215DF43E0F1C01E0CAB615B2C5D3F45D7AF42702A9D0C5F30F321E836DD6F4DDA6B8F17C8B7A278F9FDDE80B3B0960CEC0410F1ABD9326C5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Demi.woff
Preview:	wOFF.....*.....|.....v.....GPOS...l.....#....OS/2.....U...`g]|.VDMX...T.....oav.cmap.....t....cvt .....X.....fpgm...<...+...P...gasp...h.....glyf...p..Ub...,...head..j.....6...6...hhea..k....!...$...|hmtx..k0.....$7bloca..n.....maxp..q.... ... .name..r....#...A...Bpost..z$..... ...2prep..z8...../..[.x..{pTW....@.y....$.yl6...J..V.".a...B.3j+S..G.....v2.J.2V#e.+:.Lu.G.Xk.H.+J.0D....q..=.{7l..f.a.....{....{.....q.....Jd.z.....W.....mw..-..<...,...8.4....9..,....=.jM.4.k..fM..8}f..<5..4..g...s...m.V.....A.s?..a.:...8.g.....`..s.'.7jP.0Z.....`=6`#.....)..#..'{...X#.....{.c..}.5...[...kj.yU.a...l...:....{.[p.b..x.m.....6..^.....H+.7=,./y/:.NX.li...Q..;.S..R\..Y..5aM.)..s..e..).s..L}?.....vSXI.os.~ZCt....x.3...8....gJ8m.....6..:.....g....c.....-.V...x..8..s,...K.....N..~.zyn..O.4...U.a.O..2g...6...8.g\wfu...Fm.w..Z..%B...z"n..y.uX.I.E..&..#k@W..k.....U.:Q..93...f..m..g..$.8a.5=.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AvenirNext-Medium[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 33815, version 1.0
Size (bytes):	33815
Entropy (8bit):	7.9857977176837815
Encrypted:	false
MD5:	43A23A81712A5F64D86BFD2EE94E2DD6
SHA1:	793804E2D6F1345674092BEAF1090DC67E359D58
SHA-256:	D66CDC5F8FE2905D45FCE9C426D249021543CCA3C4EBD5C12B5FB67B21CD2106
SHA-512:	986FC33A03C9E8B5A60556921269BD1FCC8D842D3412B030ED122C8CBEBA2DBF40B8FA8F80686F7666873D1F8C0B5EAF90F121D96752ED121B007730AC04F9E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Medium.woff
Preview:	wOFF.....*.....},.....x.....GPOS...l.....#..=.2OS/2.....V...`f.|.VDMX...T.....o.v.cmap.....t....cvt .....U.....fpgm...8...+...P...gasp...d.....glyf...l..V....\.gCyhead..l ....6...6....hhea..l<...!...$....hmtx..l`.....#.@Mloca..oH.....maxp..s$... ... .name..sD.....@.Pgpost..{L..... ...2prep..{`...../..[.x..yl.W..?;N...W.W.#....^...j....mH|..)$-H@KT...@.....(5iTB1...J8L....Rs.(&m..C..%B...7...^.7.....7.....=8.y.;>p?2Q...o....].....yGW96v...r.....w...s.}.....Q.i..aM;5.i....L...f..6..:.q.....#8.~....PGp.....w.<^...3}. ...F...F+6...l.&l.N..A.%..[z.W.d.V.>kTvY..{..^.{.Q>...._S..+..@.mM....l.....i.nk.... ...o.....~=...~....w...5...x..uj..9.[(..9.5a.Z..):%.u.Xc.u$.u.....qR...n.+..m..Ok...7...Os.....C{...L. ...t.R..Y.....9JzLt..4W....c<t!5..7..#..i..u.<...w..Y/./1.iS.....3...=..].Lt.....n....>..._k.j".L<.%....[G5..^..a..=..tUH.....]q....3..~n.=..f..sW../.(^..4=....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AvenirNext-Regular[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 33492, version 1.0
Size (bytes):	33492
Entropy (8bit):	7.988120939904732
Encrypted:	false
MD5:	C534DE4C92BEBEE3F678DEFBC9B85EED
SHA1:	332BCFD3CB244F2BFBBCD525ED3EADB7D38C8957
SHA-256:	22444383046608AF28AF03E3CB9DFB889EB03FFD85705EF6B99103B342949F1A
SHA-512:	3239B8DEC8F1980382EEE7C086E81AAA1648FE897B7ED2BD5AB37EF24E669041293A22A971F196C3B90AEDEAACD391823D55056976747D0A67F9CBD533F47DD 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.hsappstatic.net/ui-fonts/static-1.222/fonts/AvenirNext-Regular.woff
Preview:	wOFF.....,.....{.....y.....GPOS...l...f..".....OS/2.....V...`f%{.VDMX...,.....n.v-cmap.....t....cvt .....O.....fpgm.....+...P...gasp...0.....glyf...8..U.....3.head..j. ...6...6...ghhea..k.... ...$....hmtx..k4.....JlOloca..n.....9.maxp..q.... ... ....name..r.....5.`post..z..... ...2prep..z...../..[.x..yl\W...g..x..L.&^.%..=..:.N..iK..omM....$.%*.. K.....*.*)m#(&.J...V.R...@1..l..#..`Be!=....{l...L.....;w.....y.....j..x..h.=2T.....V...M.W.....,...Wq.).5..r.iH....:M...5..G.^V.u&LM.Y....^.M.;.K.6.V..N... ....F.G1.3x...+..t...p.....B ..8....l.....q.5-.l..9.s..qk.5.Z3..jj..tJ.L.,.....m.akq....EJ....\.;....u.D.....;..{.$.=..ik.Z....5.V....,G..q...%uIh..|....&..Y.!.."W.kxp=...-..p.0G'/+)}..m.9..9.h...D7z.rO..8.C...}p5..\.:#Z...p .n.....%V.`.o..a.O..h....k..a]q.z..f....Q.|..,.....Sz...[.W..:.....=.....5..B..O7.l.NT.b..9.....+..d..fd.NSzeGS..8.@MR.....3Z.k].h..=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\earlyRequester[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Size (bytes):	10051
Entropy (8bit):	5.20917329252123
Encrypted:	false
MD5:	2BD48E12D7BE6831A42D92FCDC5DBCC8
SHA1:	AAF49A4586A74D601D19B2F0263D4E970AFBCA2D
SHA-256:	6D9E3E6503A7A86A821CA6C978D0FCB9425CA95D62715DA196714FF866ACC129
SHA-512:	CFE5C83808B9F077B368C9A8BBB105B4CDA3A9F8B339C4AA767D2CA4F1FCD2605DAD598D4BC3881796D19F7C4E9E7D984F11883218D079A0F4BA5DB20C0D3(2D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.hsappstatic.net/EmailUnsubscribeUI/static-1.3413/bundles/earlyRequester.js
Preview:	!function(e){var t={};function r(n){if(t[n])return t[n].exports;var i=t[n]={i:n,l:!1,exports:{}};e[n].call(i.exports,i,i.exports,r);i.l=!0;return i.exports}var n=[{name:"head-dlb/b undle.production.js",path:"head-dlb/static-1.49/bundle.production.js",ids:{}}];r.dlbpr=function(e,t){var i=n[e];if(!i.r){i.r=window["__webpack_require_"+i.name+"__"];if(! i.r)throw new Error("dlb "+i.name+" not loaded");i.r.linkDlb(r,i.ids)}return i.r(t)};r.m=e;r.c=t;r.d=function(e,t,n){r.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:n})};r.r =function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"});Object.defineProperty(e,"__esModule",{ value:!0})};r.t=function(e,t){1&t&&(e=r(e));if(8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var n=Object.create(null);r.r(n);Object.defineProperty(n, "default",{enumerable:!0,value:e});if(2&t&&"string"!=typeof e)for(var i in e)r.d(n,i,function(t){return e[t]}.bind(null,i));return n};r.n=fu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\bundle.production[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Size (bytes):	45069
Entropy (8bit):	5.294458316063067
Encrypted:	false
MD5:	B784CE087179C9FD939D36651AEC3549

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\bundle.production[1].js	
SHA1:	96AF4C49FA3DFE75A94B0DB8AC0867D58116A47F
SHA-256:	AF23BFBB2D154FDD2FF1E6E11AB8C215E759ABB081BF71FC5C0DC332A84E4753
SHA-512:	9793DF8A87169238D59E488483840A1B3221EDE716239B20AF13AA1F60E3E3E6D39CA7E7A3325F44500AC9795658BCEB3C1C799187BDAC1870C261FEFB155B57
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.hsappstatic.net/head-dlb/static-1.49/bundle.production.js
Preview:	!function(e){var t,r,n={};function o(t){if(n[t])return n[t].exports;var r=n[t]={i:t,l:!1,exports:{}};e[t].call(r.exports,r,r.exports,o);r.l=!0;return r.exports}o.linkDlb=function(e,n){t=e;r=n};window["__webpack_require_head-dlb/bundle.production.js__"]=o;o.dlbcr=function(e){if(!t)throw new Error("dlb consumer not properly linked");var n=r[e];if(!n)throw new Error("dlb consumer does not provide module "+e);return t(n)};o.m=e;o.c=n;o.d=function(e,t,r){o.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:r})};o.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"});Object.defineProperty(e,"__esModule",{value:!0})};o.t=function(e,t){1&t&&(e=o(e));if(8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var r=Object.create(null);o.r(r);Object.defineProperty(r,"default",{enumerable:!0,value:e});if(2&t&&"string"!=typeof e)for(var n in e)o.d(r,n,function(t){return e[t]}.bind(null,n));return r};o.n=function(e){var

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\core[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Size (bytes):	33348
Entropy (8bit):	5.296329580888088
Encrypted:	false
MD5:	00EFDCB01D5F747B6C28AF798C84F7CA
SHA1:	3BF2A08184B64D3E80970CEE91F59DE4FF13992A
SHA-256:	5F78A854E2477EB7EBDF6E4CAFD98440B70B789FCDBEE6DDD2B5FB85F3435892
SHA-512:	27931940EE7BB9C3A764ECDE62559008DFD150CF324B0066822DEF470A522F194F4A0E60DF8C6A960F28F34D3ADE0C3475A2CE4CAEC592F2FDBB79B67F81A39 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.hsappstatic.net/HeadJS/static-2.190/js/polyfills/core.js
Preview:	!function(){"use strict";function t(t,e){return e={exports:{}},t(e,e.exports),e.exports}var e,n,r,o={}.toString,i=function(t){return o.call(t).slice(8,-1)},u=Array.isArray||function(t){return"Array"==i(t)},a=function(t){return"object"==typeof t?null!==t:"function"==typeof t},c=function(t){if(void 0==t)throw TypeError("Can't call method on "+t);return t},f=function(t){return Object(c(t))},s=Math.ceil,l=Math.floor,p=function(t){return isNaN(t=+t)?0:(t>0?l:s)(t)},v=Math.min,h=function(t){return t>0?v(p(t),9007199254740991):0},d=function(t,e){if(!a(t))return t;var n,r;if(e&&"function"==typeof(n=t.toString)&&!a(r=n.call(t)))return r;if("function"==typeof(n=t.valueOf)&&!a(r=n.call(t)))return r;if(!e&&"function"==typeof(n=t.toString)&&!a(r=n.call(t)))return r;throw TypeError("Can't convert object to primitive value")},g=function(t){try{return!!t()}catch(e){return!0}},y=!g(function(){return 7!=Object.defineProperty({},"a",{get:function(){return 7}}).a}),m="object"==typeof window&&window&&windo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\doi-confirmation-container~subscription-preferences-container~subscription-unsubscribe-survey[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Size (bytes):	30652
Entropy (8bit):	5.234374628447476
Encrypted:	false
MD5:	5EC4E1135DD38304D5D30052F5C8D577
SHA1:	7347BEC029001ECEEF0DA013D231A0ED6647AACD
SHA-256:	90905752BA9D6D8A44A5D4DE4DFE3D6D22D611144B71B2F6008596846CE7343F
SHA-512:	3C4EC1D96B400F5DDFA7B40A5A4F4464AC1E2D7D245B905A1254350F2E30C6E6FF2681A081D7B140F5B797BF1DE38D8ACE2C4F74551D8946B8E0183A287E299
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.hsappstatic.net/EmailUnsubscribeUI/static-1.3413/doi-confirmation-container~subscription-preferences-container~subscription-unsubscribe-survey.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([["doi-confirmation-container~subscription-preferences-container~subscription-unsubscribe-survey"],{108:function(e,t,r){"use strict";"use es6";var n=r(1);Object.defineProperty(t,"__esModule",{value:!0});t.default=void 0;var o=n(r(109)),s=n(r(122)),u=(0,o.default)(s.default);t.default=u;e.exports=t.default},109:function(e,t,r){"use strict";"use es6";Object.defineProperty(t,"__esModule",{value:!0});t.default=void 0;var n=r(110),o=r(111),s=r(113),u=r(116),i=function(e){var t=e.useIframeRequest&&window.iframeXMLHttpRequest&&window.apiIframe&&window.apiIframe.contentDocument,r=e.useIframeRequest&&window.iframeXMLHttpRequestPromise;if(!(t||r))return(0,o.set)("Request",XMLHttpRequest)(e);var n=Object.assign({"X-HS-Referer":window.location.href},e.headers),s=(0,u.withStaticAppInfo)((0,o.set)("headers",n)(e));return r?window.iframeXMLHttpRequestPromise.then(function(e){return(0,o.set)("Request",e)(s)}).catch(function(){return(0,o.set)("Request"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\email[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Size (bytes):	37977
Entropy (8bit):	5.309740671011358
Encrypted:	false
MD5:	05C47B3FDF0C17F4DC14C73409490FB0
SHA1:	32F33ACD4C5577D6B472B6E520C2AA0ACB65293B
SHA-256:	876BBB7997FAA232FC7EF14EC0645107A375BEC44F3AE7F4D8DAB3707F9381A7
SHA-512:	24B3921F2CD80A3328AE9F12CF70C1EF0925447E8433DC4F2275E6990182BFB1C163F4A0AC83D56857291C1A3953B2695E3016C177893EEFE7708FC143136680
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\email[1].htm	
Reputation:	low
IE Cache URL:	http://https://hs-7505531.s.hubspotstarter.net/email-unsubscribe/email?product=emailStarter&d=VndZ7_57PzDHVRbf383SZtVjW3zd5WX4tcv12W3H91db3P4GWRW7_Nbz01fk4d_Vky9Mm5GrNXlW5HScjd62JJjxW6PpYRM2R6jc5N5B5t5nGKd_PV20N5J40Pn0TW8-NgKB5sJr80F6ckDhDJX0h1&v=2&email=ernie.valdez%40txdot.gov&utm_source=hs_email&utm_medium=email&utm_content=94880919&_hsenc=p2ANqtz-_t-qGyKf9L54VQYC06zkNpDt2b-DzT7t21bDE0behJn7nwzoe_XYr4aUmR4iWxXFG_bOWi31g3m_VRpgKaEsTuR5573w&_hsmi=94880919
Preview:	<!DOCTYPE html>.<html lang="en"><head><meta charset="UTF-8" />.<meta name="author" content="HubSpot, Inc." />.<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">.<link ref="preconnect" href="https://static.hsappstatic.net" crossorigin /><link rel="apple-touch-icon" sizes="180x180" href="//static.hsappstatic.net/StyleGuideUI/static-3.205/img/sprocket/apple-touch-icon.png">.<link rel="icon" type="image/png" sizes="32x32" href="//static.hsappstatic.net/StyleGuideUI/static-3.205/img/sprocket/favicon-32x32.png">.<link rel="icon" type="image/png" sizes="16x16" href="//static.hsappstatic.net/StyleGuideUI/static-3.205/img/sprocket/favicon-16x16.png"><link rel="mask-icon" href="//static.hsappstatic.net/StyleGuideUI/static-3.205/img/sprocket/safari-pinned-tab.svg" color="#FF7A59">.<meta name="msapplication-TileColor" content="#2b5797"><meta name="description" content="EmailUnsubscribeUI"/><meta name="viewport" content="width=device-width, initial-scale=1.0"/><script>var preferredLangu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\subscription-preferences-container[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Size (bytes):	40460
Entropy (8bit):	5.3472211046915605
Encrypted:	false
MD5:	D30FC7AB61160BF93BE91153AE7F29C4
SHA1:	644A8043495A092D1CED4D203B1D5FEAE288B906
SHA-256:	A3DCF7BA92974BFBF7E9CDB254CDA50F2CFC0B5E4C8B3CDE2CEB1A2BFF518CB9
SHA-512:	2481F94EE4747B383F9A681D052F0B2AB6DFA3DC148BF7AFA89CF2C9A5237D237763CAF05AFE9CE3710CC10AF5557D2E5D90D62AE24A0A4E444784808D038F8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.hsappstatic.net/EmailUnsubscribeUI/static-1.3413/subscription-preferences-container.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([["subscription-preferences-container"],{131:function(e,t,a){"use strict";"use es6";var r=a(3),n=a(1);Object.defineProperty(t,"__esModule",{value:!0});t.default=void 0;var i=n(a(9)),o=r(a(8)),s=n(a(132)),l=n(a(134)),u=function(e){var t=e.company;return o.default.createElement("div",{className:"text-center m-bottom-5"},t.logoUrl?o.default.createElement(l.default,{className:"m-x-auto m-bottom-5",src:t.logoUrl,style:{maxWidth:180}}):o.default.createElement(s.default,null,t.name))};u.propTypes={company:i.default.shape({logoUrl:i.default.string,name:i.default.string}).isRequired};var d=(0,o.memo)(u);t.default=d;e.exports=t.default},132:function(e,t,a){"use strict";"use es6";var r=a(1);Object.defineProperty(t,"__esModule",{value:!0});t.default=void 0;var n=r(a(55)),i=r(a(133)),o=(0,n.default)(i.default).attrs({as:"h1"}).withConfig({displayName:"H1",componentId:"w6rulj-0"})(["font-size:32px;font-weight:700;"]);t.default=o;e.exports=t.default}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\custom-quick-fetch[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Size (bytes):	3789
Entropy (8bit):	5.229891723432799
Encrypted:	false
MD5:	798F3FE8EA28543FAB3203AA6C4623AF
SHA1:	F31CE3E284F71EA7B83115EF68D472A1A0C6DD30
SHA-256:	6F9FE68A095DB2448F7C66EA79A78956053CFE7A4FFCC56D6F028E937CA0026E
SHA-512:	4212F72F270C8150B26AECDF0B8CE305D39F8B7B781A06A00BE7BBCB9768ED748CB5668F98B23FA1C4FFF2E1EA9C909DB6513C8125C3FB9E85B475ADB037CB8B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.hsappstatic.net/EmailUnsubscribeUI/static-1.3413/bundles/custom-quick-fetch.js
Preview:	!function(e){var t={};function r(n){if(t[n])return t[n].exports;var o=t[n]={i:n,l:!1,exports:{}};e[n].call(o.exports,o,o.exports,r);o.l=!0;return o.exports}var n=[{name:"head-dlb/bundle.production.js",path:"head-dlb/static-1.49/bundle.production.js",ids:{}}];r.dlbpr=function(e,t){var o=n[e];if(!o.r){o.r=window["__webpack_require_"+o.name+"__"];if(!o.r)throw new Error("dlb "+o.name+" not loaded");o.r.linkDlb(r,o.ids)}return o.r(t)};r.m=e;r.c=t;r.d=function(e,t,n){r.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:n})};r.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"});Object.defineProperty(e,"__esModule",{value:!0})};r.t=function(e,t){1&t&&(e=r(e));if(8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var n=Object.create(null);r.r(n);Object.defineProperty(n,"default",{enumerable:!0,value:e});if(2&t&&"string"!=typeof e)for(var o in e)r.d(n,o,function(t){return e[t]}.bind(null,o));return n};r.n=fu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\f9d051f404[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Size (bytes):	57
Entropy (8bit):	4.31817604175005
Encrypted:	false
MD5:	79F2D634CE67570918939DF10A075576
SHA1:	BA47B7DACB11250F9B1B3974B34954B188E3ECAD
SHA-256:	D10C94B6CDB747904BAEE9070F003BB45849DA46F8100B1320F286C21CBCAAA1
SHA-512:	155FAB1EC68F300DDCB948D024995539C721A2AB0FD89C220F0EFFA68C3863507CBEF806F087F5C84EAB38D4C53DA94BC893894E8FC9DED388DACFE3244E18E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\f9d051f404[1].js

Preview:	NREUM.setToken({'stn':1,'err':1,'ins':1,'cap':0,'spa':1})

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\favicon-32x32[1].png

<table>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>PNG image data, 32 x 32, 8-bit colormap, non-interlaced</td></tr>
<tr><td>Size (bytes):</td><td>1157</td></tr>
<tr><td>Entropy (8bit):</td><td>6.234045953338701</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>MD5:</td><td>5E37EA8CEC7EEE174D50087986947168</td></tr>
<tr><td>SHA1:</td><td>AA3F79209710B1C35CAA657ED1806C3A3606CEE6</td></tr>
<tr><td>SHA-256:</td><td>51FDF0D05D2D435994EA7947BDA15823B90AEB0314CA124F901F67E3D58D8D95</td></tr>
<tr><td>SHA-512:</td><td>DB4C95BCBA8FAF16BE9A57D40E3CB43D257FA91FBEBC65EF0A4E5359DAD619EAFE73D511D044A721FE909F87CBFF751106E5D626F7E5F24754ED854DDF00ABC9</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://static.hsappstatic.net/StyleGuideUI/static-3.205/img/sprocket/favicon-32x32.png</td></tr>
<tr><td>Preview:</td><td>.PNG........IHDR... ... .D.......gAMA......a.... cHRM..z&.............u0...`..:....p..Q<....PLTE....zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.
zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.
zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.
zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY.zY...(.......tRNS........'.......s..ER..Yp..,_....`!..Q...N?....z9.....4...d"..X..m..e.......a...&............M.g5.<.[T.f..1..8..6..|...%..IS.y:L..
$~.kP....IDAT8...[RA..}.T.....a.1%K...+.)......v.nj...J...n..B,.8_....y.LY...&..%.8u.......Xs..3$.j./...s8.9Q}^..7.3.xH./.\........(...,P.K......M......|.{...kUF. ....-.JDc..o.............. ;.....H."
.zz.x.....b..L.A...F...G.I.3.............Q..H...b.."=NM...$.....3..>..?W?..%..Mv27O.X._...E...r2.).2...."F</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\project[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Size (bytes):	277587
Entropy (8bit):	5.334349120952357
Encrypted:	false
MD5:	98C9D66776DF17A38C2234D1BF472DD4
SHA1:	93ACBC00D76A570BC87BA8D85DF0A62C0F804F36
SHA-256:	64365B69A15D3F7D7B58398CCD9C3BDE7658B1F749240BE6F01635FE5D8D66F1
SHA-512:	B6A1466196AD4C503C361840ED7E5E695E5C7EACD05CA091AB31EA33D5CB26F85EE0B05250EC8CEA7B5049C35EB0B06B24F8069E9DDF8324872BA8A98F28E630
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.hsappstatic.net/EmailUnsubscribeUI/static-1.3413/bundles/project.js
Preview:	window.performance&&"function"==typeof window.performance.mark&&window.performance.mark("mark_i18n_load_start");!function(e){"use strict";var t,n=Array.prototype.slice,r=function(e){return("0"+e.toString()).substr(-2)},i={day_names:["Sunday","Monday","Tuesday","Wednesday","Thursday","Friday","Saturday"],abbr_day_names:["Sun","Mon","Tue","Wed","Thu","Fri","Sat"],month_names:[null,"January","February","March","April","May","June","July","August","September","October","November","December"],abbr_month_names:[null,"Jan","Feb","Mar","Apr","May","Jun","Jul","Aug","Sep","Oct","Nov","Dec"],meridian:["AM","PM"]},a={precision:3,separator:".",delimiter:",",strip_insignificant_zeros:!0},o={unit:"$",precision:2,format:"%u%n",sign_first:!0,delimiter:",",separator:"."},l={unit:"%",precision:3,format:"%n%u",separator:".",delimiter:""},u=[null,"kb","mb","gb","tb"],s={defaultLocale:"en",locale:"en",defaultSeparator:".",placeholder:/(?:\{\{)\s?(\S*?)\s?(?:\}\})/gm,fallbacks:!1,translations:{},missingBeha

C:\Users\user\AppData\Local\Temp\~DF2D70CAC2C69ECFEC.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Size (bytes):	25441
Entropy (8bit):	0.3029020516970868
Encrypted:	false
MD5:	53006C9962728B3FE777953AAE8063B3
SHA1:	68767E54C545C8E83C4BD299507FF6CCEA81E074
SHA-256:	9F546BE16F18E792BA4967D4279DC73EC7B58DC8BFBF31B6004B35EFF44D7522
SHA-512:	38BA8E52B18E63CF91A32F4DB1CA8CA2ECF9A7DEB2763EB7E5A07D583298BDFE385048F89A9DC21EAB450E338BEB29151FA2A55150D61B26E96083C1C0C5BDE3
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF64E856541298D023.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data

C:\Users\user\AppData\Local\Temp\~DF64E856541298D023.TMP	
Size (bytes):	41050
Entropy (8bit):	1.2533935382664598
Encrypted:	false
MD5:	004D1E7411BC6A5636F24EA43F098578
SHA1:	BDA5762366E99146DB07E02C121D6A7C46207FEC
SHA-256:	1C9C9F5CB1E725803C812E00D0318905EBB8A5AB35C850097E6BA145D10054EC
SHA-512:	9B2661C3D6F09DEEFE604A8DC87671A34F2A5F71FC083BD613E7E814DF1CD3BB5F1466171D55D390DB30E9F3F7286DB6ECA581E4F233A0CEA740326D43DEC7 8
Malicious:	false
Reputation:	low
Preview:	..............................*%..H..M..{y..+.0...(................... ....*%..H..M..{y..+.0...(................... ....

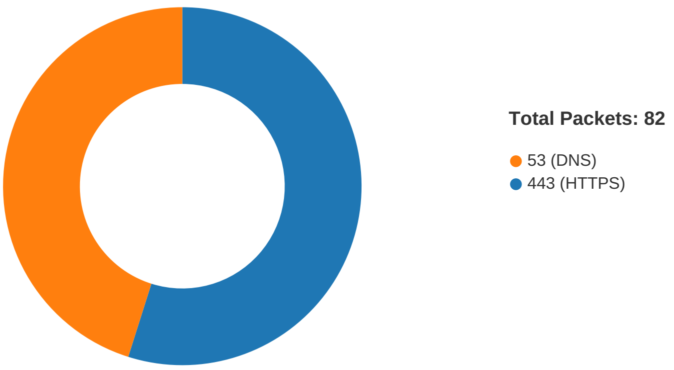
C:\Users\user\AppData\Local\Temp\~DFD91D7D91D5E864C5.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Size (bytes):	13029
Entropy (8bit):	0.4752000249261215
Encrypted:	false
MD5:	850B7002A073B5C682E194634F5A9D28
SHA1:	172B21F7AD5D0E8ABDD43B4C9AE01B139C569406
SHA-256:	9FB0ED891B6E4320C5077548D2A63F18355EB9CCC463B3708342C65FC8F88063
SHA-512:	C471E1F40A52910BBFE95602E98D8D667DB094148CC12130C1054B48AD38A74B04275993E62DE5EE41031DD1B382AF0DCC27EBC34EFF349F6C82690871E0514
Malicious:	false
Reputation:	low
Preview:	..............................*%..H..M..{y..+.0...(................... ....*%..H..M..{y..+.0...(................... ....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 10, 2020 00:39:01.462100029 CEST	49717	443	192.168.2.4	104.17.123.201
Sep 10, 2020 00:39:01.462335110 CEST	49716	443	192.168.2.4	104.17.123.201
Sep 10, 2020 00:39:01.488379955 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.488451958 CEST	443	49717	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.488498926 CEST	49716	443	192.168.2.4	104.17.123.201
Sep 10, 2020 00:39:01.489268064 CEST	49717	443	192.168.2.4	104.17.123.201
Sep 10, 2020 00:39:01.496547937 CEST	49717	443	192.168.2.4	104.17.123.201
Sep 10, 2020 00:39:01.496680975 CEST	49716	443	192.168.2.4	104.17.123.201
Sep 10, 2020 00:39:01.522545099 CEST	443	49717	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.522569895 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.524537086 CEST	443	49717	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.524559021 CEST	443	49717	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.524625063 CEST	49717	443	192.168.2.4	104.17.123.201
Sep 10, 2020 00:39:01.524669886 CEST	49717	443	192.168.2.4	104.17.123.201
Sep 10, 2020 00:39:01.525120974 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.525198936 CEST	49716	443	192.168.2.4	104.17.123.201
Sep 10, 2020 00:39:01.525207043 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.525279045 CEST	49716	443	192.168.2.4	104.17.123.201
Sep 10, 2020 00:39:01.567167044 CEST	49716	443	192.168.2.4	104.17.123.201
Sep 10, 2020 00:39:01.567260027 CEST	49717	443	192.168.2.4	104.17.123.201
Sep 10, 2020 00:39:01.573287964 CEST	49716	443	192.168.2.4	104.17.123.201
Sep 10, 2020 00:39:01.573327065 CEST	49717	443	192.168.2.4	104.17.123.201
Sep 10, 2020 00:39:01.573515892 CEST	49716	443	192.168.2.4	104.17.123.201
Sep 10, 2020 00:39:01.593465090 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.593502045 CEST	443	49717	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.593519926 CEST	443	49717	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.593542099 CEST	443	49717	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.593573093 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.593597889 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.593621969 CEST	49717	443	192.168.2.4	104.17.123.201
Sep 10, 2020 00:39:01.593646049 CEST	49716	443	192.168.2.4	104.17.123.201
Sep 10, 2020 00:39:01.593668938 CEST	49716	443	192.168.2.4	104.17.123.201
Sep 10, 2020 00:39:01.594522953 CEST	49716	443	192.168.2.4	104.17.123.201
Sep 10, 2020 00:39:01.594582081 CEST	49717	443	192.168.2.4	104.17.123.201
Sep 10, 2020 00:39:01.599348068 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.599406958 CEST	443	49717	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.599436998 CEST	443	49717	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.599478960 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.599544048 CEST	49717	443	192.168.2.4	104.17.123.201
Sep 10, 2020 00:39:01.600951910 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.601058006 CEST	49716	443	192.168.2.4	104.17.123.201
Sep 10, 2020 00:39:01.660937071 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.661115885 CEST	443	49717	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.762254000 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.762299061 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.762372017 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.762402058 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.762442112 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.762470961 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.762509108 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.762589931 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.762634039 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.762689114 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.762744904 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.762804031 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.762855053 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.762916088 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.762964010 CEST	443	49716	104.17.123.201	192.168.2.4
Sep 10, 2020 00:39:01.764861107 CEST	49716	443	192.168.2.4	104.17.123.201
Sep 10, 2020 00:39:01.765036106 CEST	49716	443	192.168.2.4	104.17.123.201
Sep 10, 2020 00:39:02.098351002 CEST	49718	443	192.168.2.4	104.17.5.210
Sep 10, 2020 00:39:02.098438025 CEST	49719	443	192.168.2.4	104.17.5.210
Sep 10, 2020 00:39:02.098572016 CEST	49720	443	192.168.2.4	104.17.5.210
Sep 10, 2020 00:39:02.098800898 CEST	49721	443	192.168.2.4	104.17.5.210

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 10, 2020 00:39:02.098824024 CEST	49722	443	192.168.2.4	104.17.5.210
Sep 10, 2020 00:39:02.098968029 CEST	49723	443	192.168.2.4	104.17.5.210
Sep 10, 2020 00:39:02.124389887 CEST	443	49720	104.17.5.210	192.168.2.4
Sep 10, 2020 00:39:02.124411106 CEST	443	49718	104.17.5.210	192.168.2.4
Sep 10, 2020 00:39:02.124418974 CEST	443	49719	104.17.5.210	192.168.2.4
Sep 10, 2020 00:39:02.124478102 CEST	443	49721	104.17.5.210	192.168.2.4
Sep 10, 2020 00:39:02.124509096 CEST	49720	443	192.168.2.4	104.17.5.210
Sep 10, 2020 00:39:02.124531984 CEST	49719	443	192.168.2.4	104.17.5.210
Sep 10, 2020 00:39:02.124548912 CEST	49718	443	192.168.2.4	104.17.5.210
Sep 10, 2020 00:39:02.124603033 CEST	443	49722	104.17.5.210	192.168.2.4
Sep 10, 2020 00:39:02.124650002 CEST	49721	443	192.168.2.4	104.17.5.210
Sep 10, 2020 00:39:02.124670029 CEST	443	49723	104.17.5.210	192.168.2.4
Sep 10, 2020 00:39:02.124690056 CEST	49722	443	192.168.2.4	104.17.5.210
Sep 10, 2020 00:39:02.124789000 CEST	49723	443	192.168.2.4	104.17.5.210
Sep 10, 2020 00:39:02.127739906 CEST	49718	443	192.168.2.4	104.17.5.210
Sep 10, 2020 00:39:02.127882004 CEST	49720	443	192.168.2.4	104.17.5.210
Sep 10, 2020 00:39:02.127995014 CEST	49719	443	192.168.2.4	104.17.5.210
Sep 10, 2020 00:39:02.128014088 CEST	49721	443	192.168.2.4	104.17.5.210
Sep 10, 2020 00:39:02.128099918 CEST	49722	443	192.168.2.4	104.17.5.210
Sep 10, 2020 00:39:02.128478050 CEST	49723	443	192.168.2.4	104.17.5.210
Sep 10, 2020 00:39:02.153498888 CEST	443	49718	104.17.5.210	192.168.2.4
Sep 10, 2020 00:39:02.153542995 CEST	443	49720	104.17.5.210	192.168.2.4
Sep 10, 2020 00:39:02.153578997 CEST	443	49719	104.17.5.210	192.168.2.4
Sep 10, 2020 00:39:02.153698921 CEST	443	49722	104.17.5.210	192.168.2.4
Sep 10, 2020 00:39:02.153726101 CEST	443	49721	104.17.5.210	192.168.2.4
Sep 10, 2020 00:39:02.154928923 CEST	443	49723	104.17.5.210	192.168.2.4
Sep 10, 2020 00:39:02.154980898 CEST	443	49718	104.17.5.210	192.168.2.4
Sep 10, 2020 00:39:02.155019999 CEST	443	49718	104.17.5.210	192.168.2.4
Sep 10, 2020 00:39:02.155056000 CEST	443	49721	104.17.5.210	192.168.2.4
Sep 10, 2020 00:39:02.155066013 CEST	49718	443	192.168.2.4	104.17.5.210
Sep 10, 2020 00:39:02.155092955 CEST	443	49721	104.17.5.210	192.168.2.4
Sep 10, 2020 00:39:02.155123949 CEST	49718	443	192.168.2.4	104.17.5.210
Sep 10, 2020 00:39:02.155132055 CEST	443	49719	104.17.5.210	192.168.2.4
Sep 10, 2020 00:39:02.155167103 CEST	443	49719	104.17.5.210	192.168.2.4
Sep 10, 2020 00:39:02.155205011 CEST	443	49720	104.17.5.210	192.168.2.4
Sep 10, 2020 00:39:02.155205011 CEST	49721	443	192.168.2.4	104.17.5.210

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 10, 2020 00:38:54.969554901 CEST	58963	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:38:54.996505976 CEST	53	58963	8.8.8.8	192.168.2.4
Sep 10, 2020 00:38:55.828548908 CEST	64705	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:38:55.855029106 CEST	53	64705	8.8.8.8	192.168.2.4
Sep 10, 2020 00:38:56.992173910 CEST	61585	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:38:57.018690109 CEST	53	61585	8.8.8.8	192.168.2.4
Sep 10, 2020 00:39:00.146356106 CEST	63540	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:39:00.179078102 CEST	53	63540	8.8.8.8	192.168.2.4
Sep 10, 2020 00:39:01.400141954 CEST	50757	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:39:01.448961973 CEST	53	50757	8.8.8.8	192.168.2.4
Sep 10, 2020 00:39:01.839993000 CEST	59058	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:39:01.866652012 CEST	53	59058	8.8.8.8	192.168.2.4
Sep 10, 2020 00:39:02.977904081 CEST	53809	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:39:03.004566908 CEST	53	53809	8.8.8.8	192.168.2.4
Sep 10, 2020 00:39:03.945828915 CEST	52224	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:39:03.983390093 CEST	53	52224	8.8.8.8	192.168.2.4
Sep 10, 2020 00:39:05.175510883 CEST	57637	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:39:05.211776972 CEST	53	57637	8.8.8.8	192.168.2.4
Sep 10, 2020 00:39:05.389127970 CEST	63419	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:39:05.415533066 CEST	53	63419	8.8.8.8	192.168.2.4
Sep 10, 2020 00:39:14.650372028 CEST	54357	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:39:14.677853107 CEST	53	54357	8.8.8.8	192.168.2.4
Sep 10, 2020 00:39:18.281603098 CEST	60328	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:39:18.309107065 CEST	53	60328	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 10, 2020 00:39:22.508301973 CEST	49936	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:39:22.544783115 CEST	53	49936	8.8.8.8	192.168.2.4
Sep 10, 2020 00:39:27.425578117 CEST	52456	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:39:27.458596945 CEST	53	52456	8.8.8.8	192.168.2.4
Sep 10, 2020 00:39:30.153964996 CEST	65061	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:39:30.181243896 CEST	53	65061	8.8.8.8	192.168.2.4
Sep 10, 2020 00:39:30.845165014 CEST	58776	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:39:30.873303890 CEST	53	58776	8.8.8.8	192.168.2.4
Sep 10, 2020 00:39:31.169653893 CEST	65061	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:39:31.197227001 CEST	53	65061	8.8.8.8	192.168.2.4
Sep 10, 2020 00:39:31.855694056 CEST	58776	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:39:31.881905079 CEST	53	58776	8.8.8.8	192.168.2.4
Sep 10, 2020 00:39:32.184206009 CEST	65061	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:39:32.211070061 CEST	53	65061	8.8.8.8	192.168.2.4
Sep 10, 2020 00:39:32.874222040 CEST	58776	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:39:32.902528048 CEST	53	58776	8.8.8.8	192.168.2.4
Sep 10, 2020 00:39:34.714165926 CEST	65061	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:39:34.743712902 CEST	53	65061	8.8.8.8	192.168.2.4
Sep 10, 2020 00:39:35.006392002 CEST	58776	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:39:35.035677910 CEST	53	58776	8.8.8.8	192.168.2.4
Sep 10, 2020 00:39:38.719837904 CEST	65061	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:39:38.746623993 CEST	53	65061	8.8.8.8	192.168.2.4
Sep 10, 2020 00:39:39.012474060 CEST	58776	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:39:39.039653063 CEST	53	58776	8.8.8.8	192.168.2.4
Sep 10, 2020 00:39:44.532047033 CEST	52994	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:39:44.559578896 CEST	53	52994	8.8.8.8	192.168.2.4
Sep 10, 2020 00:40:14.822139025 CEST	56954	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:40:14.909626007 CEST	53	56954	8.8.8.8	192.168.2.4
Sep 10, 2020 00:40:15.558207989 CEST	63252	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:40:15.585365057 CEST	53	63252	8.8.8.8	192.168.2.4
Sep 10, 2020 00:40:16.415983915 CEST	63343	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:40:16.443203926 CEST	53	63343	8.8.8.8	192.168.2.4
Sep 10, 2020 00:40:16.560168982 CEST	49290	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:40:16.586366892 CEST	53	49290	8.8.8.8	192.168.2.4
Sep 10, 2020 00:40:16.997266054 CEST	58969	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:40:17.024158001 CEST	53	58969	8.8.8.8	192.168.2.4
Sep 10, 2020 00:40:17.138309956 CEST	60749	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:40:17.187232018 CEST	53	60749	8.8.8.8	192.168.2.4
Sep 10, 2020 00:40:17.531666040 CEST	60322	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:40:17.558922052 CEST	53	60322	8.8.8.8	192.168.2.4
Sep 10, 2020 00:40:18.526757002 CEST	52297	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:40:18.554455996 CEST	53	52297	8.8.8.8	192.168.2.4
Sep 10, 2020 00:40:19.064805031 CEST	49932	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:40:19.091681957 CEST	53	49932	8.8.8.8	192.168.2.4
Sep 10, 2020 00:40:19.743324995 CEST	57715	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:40:19.770258904 CEST	53	57715	8.8.8.8	192.168.2.4
Sep 10, 2020 00:40:20.412408113 CEST	60858	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:40:20.439315081 CEST	53	60858	8.8.8.8	192.168.2.4
Sep 10, 2020 00:40:21.195039988 CEST	60271	53	192.168.2.4	8.8.8.8
Sep 10, 2020 00:40:21.222410917 CEST	53	60271	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 10, 2020 00:39:01.400141954 CEST	192.168.2.4	8.8.8.8	0xbc40	Standard query (0)	hs-7505531.s.hubspotstarter.net	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:01.839993000 CEST	192.168.2.4	8.8.8.8	0x52c5	Standard query (0)	static.hsappstatic.net	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:02.977904081 CEST	192.168.2.4	8.8.8.8	0x7fec	Standard query (0)	api.hubspot.com	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:03.945828915 CEST	192.168.2.4	8.8.8.8	0x549b	Standard query (0)	f.hubspotusercontent30.net	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:05.175510883 CEST	192.168.2.4	8.8.8.8	0x3352	Standard query (0)	js-agent.newrelic.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 10, 2020 00:39:05.389127970 CEST	192.168.2.4	8.8.8.8	0x919d	Standard query (0)	bam.nr-data.net	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:18.281603098 CEST	192.168.2.4	8.8.8.8	0xc1f8	Standard query (0)	static.hsa ppstatic.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 10, 2020 00:39:01.448961973 CEST	8.8.8.8	192.168.2.4	0xbc40	No error (0)	hs-7505531 .s.hubspot starter.net		104.17.123.201	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:01.448961973 CEST	8.8.8.8	192.168.2.4	0xbc40	No error (0)	hs-7505531 .s.hubspot starter.net		104.17.120.201	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:01.448961973 CEST	8.8.8.8	192.168.2.4	0xbc40	No error (0)	hs-7505531 .s.hubspot starter.net		104.17.124.201	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:01.448961973 CEST	8.8.8.8	192.168.2.4	0xbc40	No error (0)	hs-7505531 .s.hubspot starter.net		104.17.121.201	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:01.448961973 CEST	8.8.8.8	192.168.2.4	0xbc40	No error (0)	hs-7505531 .s.hubspot starter.net		104.17.122.201	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:01.866652012 CEST	8.8.8.8	192.168.2.4	0x52c5	No error (0)	static.hsa ppstatic.net		104.17.5.210	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:01.866652012 CEST	8.8.8.8	192.168.2.4	0x52c5	No error (0)	static.hsa ppstatic.net		104.17.8.210	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:01.866652012 CEST	8.8.8.8	192.168.2.4	0x52c5	No error (0)	static.hsa ppstatic.net		104.17.6.210	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:01.866652012 CEST	8.8.8.8	192.168.2.4	0x52c5	No error (0)	static.hsa ppstatic.net		104.17.9.210	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:01.866652012 CEST	8.8.8.8	192.168.2.4	0x52c5	No error (0)	static.hsa ppstatic.net		104.17.7.210	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:03.004566908 CEST	8.8.8.8	192.168.2.4	0x7fec	No error (0)	api.hubspot.com		104.19.154.83	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:03.004566908 CEST	8.8.8.8	192.168.2.4	0x7fec	No error (0)	api.hubspot.com		104.19.155.83	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:03.983390093 CEST	8.8.8.8	192.168.2.4	0x549b	No error (0)	f.hubspotu sercontent30.net		104.16.185.114	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:03.983390093 CEST	8.8.8.8	192.168.2.4	0x549b	No error (0)	f.hubspotu sercontent30.net		104.16.184.114	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:05.211776972 CEST	8.8.8.8	192.168.2.4	0x3352	No error (0)	js-agent.n ewrelic.com	f4.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Sep 10, 2020 00:39:05.415533066 CEST	8.8.8.8	192.168.2.4	0x919d	No error (0)	bam.nr-data.net		162.247.242.19	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:05.415533066 CEST	8.8.8.8	192.168.2.4	0x919d	No error (0)	bam.nr-data.net		162.247.242.18	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:05.415533066 CEST	8.8.8.8	192.168.2.4	0x919d	No error (0)	bam.nr-data.net		162.247.242.20	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:05.415533066 CEST	8.8.8.8	192.168.2.4	0x919d	No error (0)	bam.nr-data.net		162.247.242.21	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:18.309107065 CEST	8.8.8.8	192.168.2.4	0xc1f8	No error (0)	static.hsa ppstatic.net		104.17.5.210	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:18.309107065 CEST	8.8.8.8	192.168.2.4	0xc1f8	No error (0)	static.hsa ppstatic.net		104.17.8.210	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:18.309107065 CEST	8.8.8.8	192.168.2.4	0xc1f8	No error (0)	static.hsa ppstatic.net		104.17.6.210	A (IP address)	IN (0x0001)
Sep 10, 2020 00:39:18.309107065 CEST	8.8.8.8	192.168.2.4	0xc1f8	No error (0)	static.hsa ppstatic.net		104.17.9.210	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 10, 2020 00:39:18.309107065 CEST	8.8.8.8	192.168.2.4	0xc1f8	No error (0)	static.hsappstatic.net		104.17.7.210	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
Sep 10, 2020 00:39:01.524559021 CEST	104.17.123.201	443	192.168.2.4	49717	CN=hubspotstarter.net, 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 Jul 01 02:00:00 CEST 2020	Thu Jul 01 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Sep 10, 2020 00:39:01.525207043 CEST	104.17.123.201	443	192.168.2.4	49716	CN=hubspotstarter.net, 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 Jul 01 02:00:00 CEST 2020	Thu Jul 01 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Sep 10, 2020 00:39:02.155019999 CEST	104.17.5.210	443	192.168.2.4	49718	CN=hsappstatic.net, 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	Sun Jul 05 02:00:00 CEST 2020	Mon Jul 05 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Sep 10, 2020 00:39:02.155092955 CEST	104.17.5.210	443	192.168.2.4	49721	CN=hsappstatic.net, 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	Sun Jul 05 02:00:00 CEST 2020	Mon Jul 05 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Sep 10, 2020 00:39:02.155167103 CEST	104.17.5.210	443	192.168.2.4	49719	CN=hsappstatic.net, 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	Sun Jul 05 02:00:00 CEST 2020	Mon Jul 05 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Sep 10, 2020 00:39:02.155237913 CEST	104.17.5.210	443	192.168.2.4	49720	CN=hsappstatic.net, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	Sun Jul 05 02:00:00 CEST 2020	Mon Jul 05 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Sep 10, 2020 00:39:02.155647039 CEST	104.17.5.210	443	192.168.2.4	49722	CN=hsappstatic.net, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	Sun Jul 05 02:00:00 CEST 2020	Mon Jul 05 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Sep 10, 2020 00:39:02.157685995 CEST	104.17.5.210	443	192.168.2.4	49723	CN=hsappstatic.net, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	Sun Jul 05 02:00:00 CEST 2020	Mon Jul 05 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Sep 10, 2020 00:39:03.276314974 CEST	104.19.154.83	443	192.168.2.4	49725	CN=hubspot.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	Mon Jul 27 02:00:00 CEST 2020	Tue Jul 27 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Sep 10, 2020 00:39:03.279181004 CEST	104.19.154.83	443	192.168.2.4	49724	CN=hubspot.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	Mon Jul 27 02:00:00 CEST 2020	Tue Jul 27 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Sep 10, 2020 00:39:04.074472904 CEST	104.16.185.114	443	192.168.2.4	49726	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	Sun Aug 16 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Mon Aug 16 14:00:00 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		
Sep 10, 2020 00:39:04.077461958 CEST	104.16.185.114	443	192.168.2.4	49727	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sun Aug 16 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Mon Aug 16 14:00:00 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		
Sep 10, 2020 00:39:05.707555056 CEST	162.247.242.19	443	192.168.2.4	49730	CN=*.nr-data.net, O="New Relic, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 05 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Tue Feb 08 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023	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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Sep 10, 2020 00:39:05.709343910 CEST	162.247.242.19	443	192.168.2.4	49731	CN=*.nr-data.net, O="New Relic, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 05 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Tue Feb 08 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023	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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Sep 10, 2020 00:39:18.372680902 CEST	104.17.5.210	443	192.168.2.4	49735	CN=hsappstatic.net, 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	Sun Jul 05 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Mon Jul 05 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
						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: 6664 Parent PID: 796

General

Start time:	00:38:59
Start date:	10/09/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7fb9a0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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: 6716 Parent PID: 6664

General

Start time:	00:38:59
Start date:	10/09/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6664 CREDAT:17410 /prefetch:2
Imagebase:	0xf70000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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

Disassembly