



ID: 368837
Cookbook: browseurl.jbs
Time: 17:34:22
Date: 15/03/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report https://ph-northwestmi.as.me/efreechurchdose1covid20210310 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 11
Public 11
General Information 11
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASN 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 34
No static file info 34
Network Behavior 35
Network Port Distribution 35
TCP Packets 35
UDP Packets 36
DNS Queries 38
DNS Answers 38
HTTPS Packets 39
Code Manipulations 46
Statistics 46
Behavior 46
System Behavior 46
Analysis Process: iexplore.exe PID: 5408 Parent PID: 792 46
General 46

File Activities 47
Registry Activities 47
Analysis Process: iexplore.exe PID: 5608 Parent PID: 5408 47
General 47
File Activities 47
Registry Activities 47
Disassembly 47

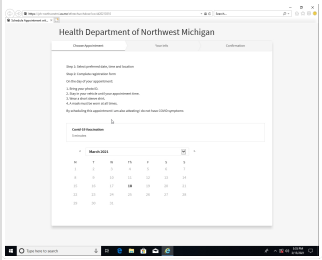
Analysis Report https://ph-northwestmi.as.me/efreechur…

Overview

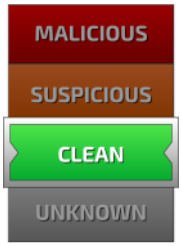
General Information

Sample URL:	http://https://ph-northwestmi.as.me/efreechurchdose1covid20210310
Analysis ID:	368837
Infos:	

Most interesting Screenshot:



Detection

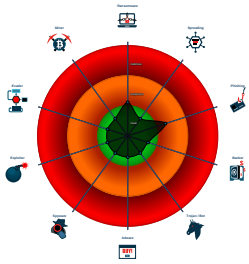


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- HTML body contains low number of …
- Suspicious form URL found

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5408 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5608 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5408 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

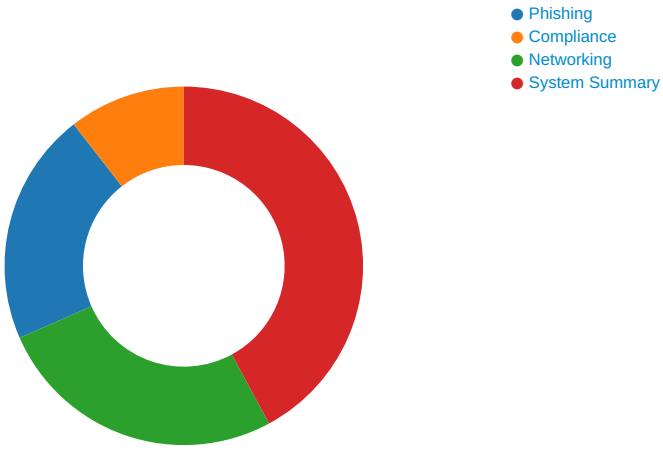
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright Joe Security LLC 2021



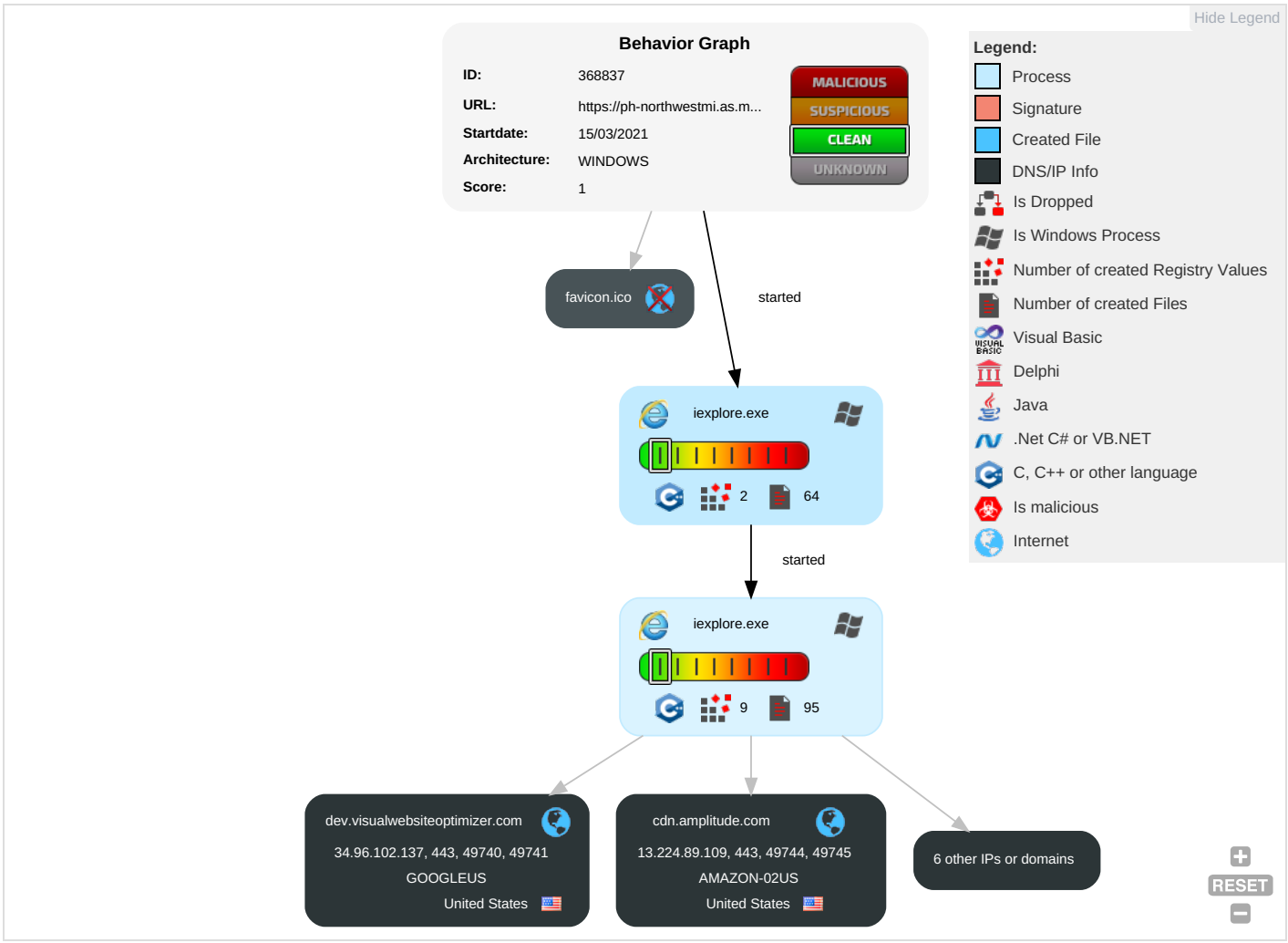
Click to jump to signature section

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 1	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

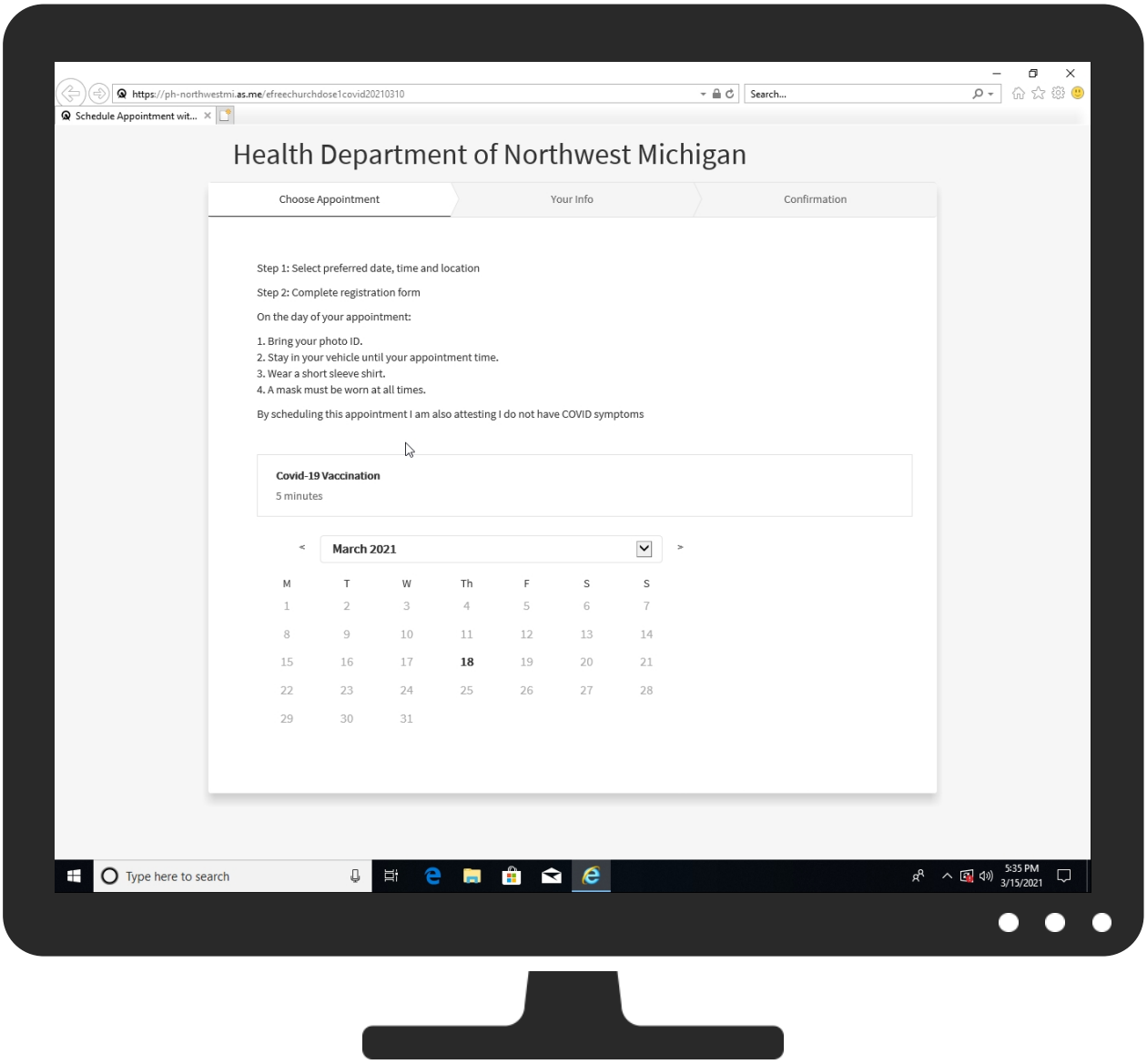


Screenshots

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://ph-northwestmi.as.me/efreechurchdose1covid20210310	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://popper.js.org	1%	Virustotal		Browse
http://https://popper.js.org	0%	Avira URL Cloud	safe	
http://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://www.optimo.chhttps://www.optimo.ch/information-eula	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://https://atomiks.github.io/tippyjs/getting-started/	0%	Avira URL Cloud	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://ph-northwduling.com/?utm_campaign=acuity&utm_medium=referral&utm_source=s	0%	Avira URL Cloud	safe	
http://https://trustarc.mgr.consensu.org/	0%	URL Reputation	safe	
http://https://trustarc.mgr.consensu.org/	0%	URL Reputation	safe	
http://https://trustarc.mgr.consensu.org/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
secure.acuityscheduling.com	52.89.211.128	true	false		high
api.amplitude.com	54.184.84.60	true	false		high
dev.visualwebsiteoptimizer.com	34.96.102.137	true	false		high
cdn.amplitude.com	13.224.89.109	true	false		high
ph-northwestmi.as.me	35.160.170.4	true	false		high
www.acuityscheduling.com	35.160.170.4	true	false		high
consent.trustarc.com	13.224.94.16	true	false		high
cdn-marketing.acuityscheduling.com	unknown	unknown	false		high
favicon.ico	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://ph-northwestmi.as.me/efreechurchdose1covid20210310#selectedTimes	false		high
http://https://www.acuityscheduling.com/?utm_campaign=acuity&utm_medium=referral&utm_source=scheduling	false		high
http://https://ph-northwestmi.as.me/efreechurchdose1covid20210310	false		high
http://https://ph-northwestmi.as.me/client-login.php?owner=21613168&PHPSESSID=isj29ml5484939e2lnhrbbsir3&returnUrl=%2Fschedule.php%3Fowner%3D21613168%26calendarID%3D4953566	false		high
http://https://ph-northwestmi.as.me/schedule.php?owner=21613168&calendarID=4953566	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontawesome.io	schedule[1].css.2.dr	false		high
http://https://ph-northw.as.me/efreechurchdose1covid20210310#selectedTimes29ml5484939e	{747EC0F3-85EF-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://popper.js.org	tippy[1].js.2.dr	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/screen-organize.png	TV4F7E56.htm.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/logo-stripe.svg	TV4F7E56.htm.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/screen-control.png	TV4F7E56.htm.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/site-schooner-coaching.svg	TV4F7E56.htm.2.dr	false		high
http://https://dev.visualwebsiteoptimizer.com/v.gif?cd=	j[1].js0.2.dr, j[1].js.2.dr	false		high
http://https://www.squarespace.com/privacy	TV4F7E56.htm.2.dr	false		high
http://https://www.acuityscheduling.com/?utm_campaign=acl	{747EC0F3-85EF-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/launch-iphone-xr.png	TV4F7E56.htm.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/js/swipe.js	TV4F7E56.htm.2.dr, login[1].htm.2.dr	false		high
http://https://www.optimo.ch/information-eula	get[1].2.dr	false		high

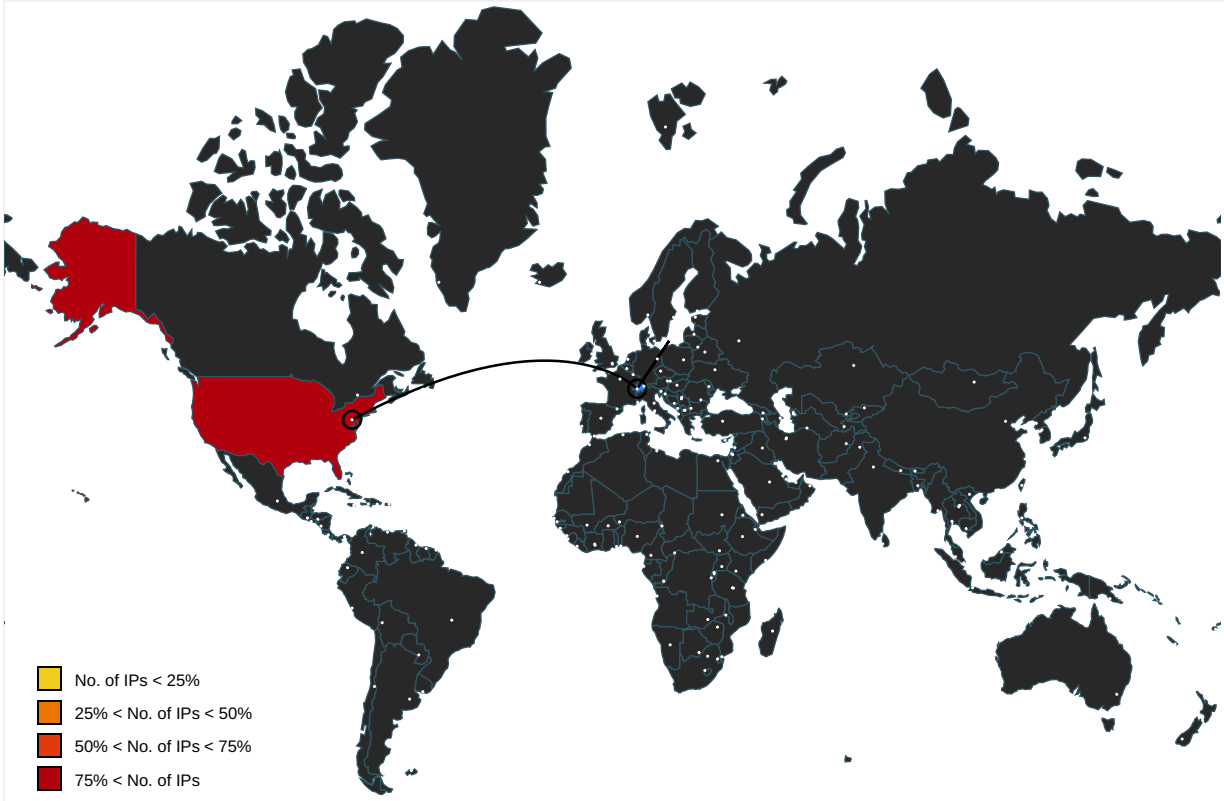
Copyright Joe Security LLC 2021

Name	Source	Malicious	Antivirus Detection	Reputation
http://consent.trustarc.com/bannermsg?	notice[1].js.2.dr, notice[2].js.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/launch-ipad-pro-12.9.png	TV4F7E56.htm.2.dr	false		high
http://https://dev.visualwebsiteoptimizer.com/e.gif?s=mode_det&e=	j[1].js0.2.dr, j[1].js.2.dr	false		high
http://https://ph-northwestmi.as.me/favicon.icoj	imagestore.dat.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/launch-ipad-mini-9.7.png	TV4F7E56.htm.2.dr	false		high
http://https://gist.github.com/71302de5c334d16fa768	schedule[1].css.2.dr	false		high
http://getbootstrap.com)	schedule[1].css.2.dr	false	• Avira URL Cloud: safe	low
http://opensource.org/licenses/MIT).	tippy[1].js.2.dr	false		high
http://https://dev.visualwebsiteoptimizer.com/j.php?mode=	j[1].js0.2.dr, j[1].js.2.dr	false		high
http://https://fife-hawk-s476.squarespace.com/	TV4F7E56.htm.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/down.svg	TV4F7E56.htm.2.dr	false		high
http://https://help.acuityscheduling.com/hc/	TV4F7E56.htm.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/launch-iphone-6s-7-8.png	TV4F7E56.htm.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/logo-ga.svg	TV4F7E56.htm.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/js/tippy.js	TV4F7E56.htm.2.dr, login[1].htm.2.dr	false		high
http://https://app.acuityscheduling.com/schedule.php?owner=21613168	schedule[1].htm.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/font/Clarkson-Light.woff2	TV4F7E56.htm.2.dr	false		high
http://https://clover-trombone-al4y.squarespace.com/home	TV4F7E56.htm.2.dr	false		high
http://https://www.squarespace.com/terms-of-service	TV4F7E56.htm.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/logo-square.svg	TV4F7E56.htm.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/launch-ipad-pro-11.png	TV4F7E56.htm.2.dr	false		high
http://https://www.acuityscheduling.com/?utm_campaign=acuity&utm_medium=referral&utm_source=scheduling3&ret	~DF1208AB93F940F0FF.TMP.1.dr	false		high
http://https://www.optimo.chhttps://www.optimo.ch/information-eula	get[1].2.dr, get[1]0.2.dr	false	• Avira URL Cloud: safe	unknown
http://consent-pref.trustarc.com/?type=squarespace2	notice[1].js.2.dr, notice[2].js.2.dr	false		high
http://consent.trustarc.com/	notice[2].js.2.dr	false		high
http://https://ph-northwestmi.as.me/schedule.php?owner=21613168&calendarID=4953566	~DF1208AB93F940F0FF.TMP.1.dr	false		high
http://https://ph-northwestmi.as.me/client-login.php?owner=21613168&PHPSESSID=isj29ml5484939e2lnhrbbsir3&re	~DF1208AB93F940F0FF.TMP.1.dr	false		high
http://https://help.acuityscheduling.com/hc/requests/new	TV4F7E56.htm.2.dr	false		high
http://https://atomiks.github.io/tippyjs/getting-started/	tippy[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cct.google/taggy/agent.js	gtm[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ph-northwestmi.as.me/efreechurchdose1covid20210310#selectedTimes	~DF1208AB93F940F0FF.TMP.1.dr	false		high
http://https://ph-northw.as.me/schedule.php?owner=21613168&calendarID=4953566Root	{747EC0F3-85EF-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://www.instagram.com/acuityscheduling/	TV4F7E56.htm.2.dr	false		high
http://https://www.acuityscheduling.com/?utm_campaign=acuity&utm_medium=referral&utm_source=scheduling	~DF1208AB93F940F0FF.TMP.1.dr	false		high
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	schedule[1].css.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/left.svg	TV4F7E56.htm.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/font/Clarkson-Medium.woff2	TV4F7E56.htm.2.dr	false		high
http://https://consent.trustarc.com/log	notice[1].js.2.dr	false		high
http://https://AcuityScheduling.com	TV4F7E56.htm.2.dr	false		high
http://https://secure.acuityscheduling.com/	{747EC0F4-85EF-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/site-whiskey-business.svg	TV4F7E56.htm.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/support	TV4F7E56.htm.2.dr	false		high
http://https://www.squarespace.com/?utm_source=acuityscheduling.com&utm_medium=referral&utm_campaign=homepa	TV4F7E56.htm.2.dr	false		high
http://https://secure.acuityscheduling.com/login.php	TV4F7E56.htm.2.dr, login[1].htm.2.dr, ~DF904815EF7ED92817.TMP.1.dr	false		high
http://https://pelican-orb-pnxf.squarespace.com/	TV4F7E56.htm.2.dr	false		high
http://https://www.squarespace.com/?source=acuityfooter	TV4F7E56.htm.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/img/brand/logo-og.png	TV4F7E56.htm.2.dr	false		high
http://https://app.acuityscheduling.com/schedule.php?owner=21613168&q=efreechurchdose1covid20210310&calenda	efreechurchdose1covid20210310[1].htm.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/support.jpg	TV4F7E56.htm.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/launch-ipad-pro-10.5.png	TV4F7E56.htm.2.dr	false		high
http://https://s.pinimg.com/ct/core.js	gtm[1].js.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/logo-zapier.svg	TV4F7E56.htm.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/built/csp/schedule.css?v=c1a593	schedule[1].htm.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/site-gavins-goodies.svg	TV4F7E56.htm.2.dr	false		high
http://https://api-js-log.trustarc.com/error	notice[1].js.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/screen-collect.png	TV4F7E56.htm.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/screen-collect	TV4F7E56.htm.2.dr	false		high
http://https://www.acuityscheduling.com/?utm_campaign=acuity&utm_medium=referral&utm_source=schedulingHAcui	~DF1208AB93F940F0FF.TMP.1.dr	false		high
http://getbootstrap.com/customize/?id=71302de5c334d16fa768)	schedule[1].css.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/launch-iphone-xs-max.png	TV4F7E56.htm.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/logo-paypal.svg	TV4F7E56.htm.2.dr	false		high
http://https://app.vwo.com/visitor-behavior-analysis/dist/codechecker/cc.min.js?r=	j[1].js0.2.dr, j[1].js.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/built/csp/schedule.all.js?v=c1a593	schedule[1].htm.2.dr	false		high
http://https://www.optimo.ch/information-eulaClarkson	get[1].2.dr	false		high
http://https://acuityscheduling.com/login.php	login[1].htm.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/site-llama-ste.svg	TV4F7E56.htm.2.dr	false		high
http://https://ph-northwduling.com/?utm_campaign=acuity&utm_medium=referral&utm_source=s	{747EC0F3-85EF-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://ph-northwestmi.as.me/efreechurchdose1covid20210310#selectedTimes29ml5484939e2lnhrbbsir3&retu	~DF1208AB93F940F0FF.TMP.1.dr	false		high
http://https://carnation-cardioid-znps.squarespace.com/	TV4F7E56.htm.2.dr	false		high
http://status.acuityscheduling.com/	TV4F7E56.htm.2.dr	false		high
http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/site-under-pressure.svg	TV4F7E56.htm.2.dr	false		high
http://https://consent.trustarc.com/	notice[2].js.2.dr	false		high
http://consent.trustarc.com/noticemsg?	notice[1].js.2.dr, notice[2].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://app.acuityscheduling.com/schedule.php?owner=21613168&calendarID=4953566	schedule[1].htm.2.dr	false		high
http://https://acuityscheduling.com/blog	TV4F7E56.htm.2.dr	false		high
http://https://consent.trustarc.com/get?name=icon_cross_large.svg	notice[1].js.2.dr, notice[2].js.2.dr	false		high
http://https://developers.acuityscheduling.com/	TV4F7E56.htm.2.dr	false		high
http://https://ph-northwestmi.as.me/efreechurchdose1covid20210310Root	{747EC0F3-85EF-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://acuityscheduling.com/	TV4F7E56.htm.2.dr	false		high
http://https://trustarc.mgr.consensu.org/	notice[1].js.2.dr, notice[2].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://help.acuityscheduling.com/hc/en-us/requests/new	login[1].js.2.dr	false		high
http://https://sponge-dachshund-jd56.squarespace.com/	TV4F7E56.htm.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.96.102.137	dev.visualwebsiteoptimizer.com	United States		15169	GOOGLEUS	false
52.89.211.128	secure.acuityscheduling.com	United States		16509	AMAZON-02US	false
54.184.84.60	api.amplitude.com	United States		16509	AMAZON-02US	false
13.224.89.109	cdn.amplitude.com	United States		16509	AMAZON-02US	false
13.224.94.16	consent.trustarc.com	United States		16509	AMAZON-02US	false
35.160.170.4	ph-northwestmi.as.me	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	368837
Start date:	15.03.2021
Start time:	17:34:22

Copyright Joe Security LLC 2021

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://ph-northwestmi.as.me/efreechurchdose1covid20210310
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	8
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:	clean1.win@3/65@9/6
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://ph-northwestmi.as.me/schedule.php?owner=21613168&calendarID=4953566 • Browsing link: https://ph-northwestmi.as.me/client-login.php?owner=21613168&PHPSESSID=isj29ml5484939e2lnhrbbsir3&returnUrl=%2Fschedule.php%3Fowner%3D21613168%26calendarID%3D4953566 • Browsing link: https://ph-northwestmi.as.me/efreechurchdose1covid20210310#selectedTimes • Browsing link: https://www.acuityscheduling.com/?utm_campaign=acuity&utm_medium=referral&utm_source=scheduling
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 23.211.6.115, 13.88.21.125, 104.43.139.144, 172.227.100.57, 151.101.2.217, 151.101.66.217, 151.101.130.217, 151.101.194.217, 172.217.22.202, 216.58.207.163, 13.64.90.137, 104.42.151.234, 172.217.20.234, 216.58.207.136, 152.199.19.161, 51.104.139.180, 104.84.56.60 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, go.microsoft.com, www.googletagmanager.com, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, fonts.googleapis.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, fonts.gstatic.com, ajax.googleapis.com, ie9comview.vo.msecnd.net, www-googletagmanager.l.google.com, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, store-images.s-microsoft.com, i3.shared.global.fastly.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.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\HL5RDMJ5\secure.acuityscheduling[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Reputation:	low
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\UD03UG22\ph-northwestmi.as[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	111
Entropy (8bit):	4.73614701232222
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsHKJMEWBCzygTqqFf3AlUdYq9qSQRM0LKb:JFK1rUF2MEWBCiq93AydlQRib
MD5:	535F52270FFA7711FB3C84AB9EBCFA31
SHA1:	9B02744C6443D8749EFBB0F99DA6528DF581366C

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\UD03UG22\ph-northwestmi.as[1].xml	
SHA-256:	1E13383BCA33D0AC81831E8C871DA22E46DC7E0FAD6EB83419C1A30D6EE7BD86
SHA-512:	4DC4015FC1DE60DB47FAA9D384725188EA1C555663FCDE331707F6CA3A6E2C7185E879E17933D1682A7281A3FE0B1C2E0FBE97D94313F4B073255A9886009E34
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="algoliasearch-client-js" value="{}" ltime="949118032" htime="30874108" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\XKZEGMZ4\www.acuityscheduling[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	35080
Entropy (8bit):	5.1300231200138695
Encrypted:	false
SSDEEP:	384:VMjdVMj4VMj4VMjs0VMjsD0VMjsHGMUjVMjsHGMUjVMjshVGMUPZhAPZhABj3:6d6464636d6Hj6Hj6W+PDwDO
MD5:	24D30E4728FD121EBD8A65D2DB05C15C
SHA1:	1B23488F0B72CB01C841C3F140B58BB991D78AEC
SHA-256:	D6156A33B255F6640FFBC6C18F5BB103211B272EEA3299BCC435836A7A14A304
SHA-512:	8DA9F3FC4772AAEF8D711A27E51DFD2D8D92467A51679C14A7F486355CDB32D668131287168F04F1D2DB1AECB8A77E07F3ADAFD433184442C9144450D4319B7
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="Mon Mar 15 2021 17:35:34 GMT-0700 (Pacific Daylight Time)" value="Mon Mar 15 2021 17:35:34 GMT-0700 (Pacific Daylight Time)" ltime="1188428032" htime="30874108" /></root><root></root><root><item name="amplitude_unsent_5bf377fa898a63e32d803ce376dbf310_acuity" value="[]" ltime="1188708032" htime="30874108" /></root><root><item name="amplitude_unsent_5bf377fa898a63e32d803ce376dbf310_acuity" value="[]" ltime="1188708032" htime="30874108" /><item name="amplitude_unsent_identify_5bf377fa898a63e32d803ce376dbf310_acuity" value="[]" ltime="1188708032" htime="30874108" /></root><root><item name="amplitude_unsent_5bf377fa898a63e32d803ce376dbf310_acuity" value="[]" ltime="1188748032" htime="30874108" /><item name="amplitude_unsent_identify_5bf377fa898a63e32d803ce376dbf310_acuity" value="[]" ltime="1188708032" htime="30874108" /></root><root><item name="amplitude_unsent_5bf377fa898a63e32d803ce376dbf310_acuity" value="[]" ltime="1188748032" htime="30874108" /><item nam

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{747EC0F1-85EF-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	35928
Entropy (8bit):	1.9108860114254929
Encrypted:	false
SSDEEP:	96:rXZkVZR2pWugtujfuJRMuWuKu0fuKMruK0fu/bX:rXZ4ZR2pWLt0fERMrT7fXMr/0fabX
MD5:	7EAD4C0E3720839CB543D8C87FD10711
SHA1:	66B69F61384484C974C164340FBCB3FF58CDD48D
SHA-256:	ADB33C89C5061B7ACDCC3C3939CFFA270F71953FBCB4116BC9F4FCA9E208F1AB
SHA-512:	0CF5975F2962488D440D0C6C3D669CABD49F5DAB392ED0E83865AF28D197D0251DEF59524112A9020246AA5DF9372D77A5BBB39C539381016210E50F39F64CAD
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\{747EC0F3-85EF-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	87728
Entropy (8bit):	2.590607330384925
Encrypted:	false
SSDEEP:	1536:E1s3SDb1E+Ro2SJUeLJ/QDwsmqmKCwirpO:E1s3SDb1E+Ro2SJUeLJ/Q0sR/kE
MD5:	A9CBBED1140185B5180A08C6E2FEC86C
SHA1:	45B69F92CFFE70919B75854303D35AE136E46E21
SHA-256:	7EC5A7B92AF0468B5228F6493A0EC98A170B236675ECFD4FDF813EBD607CCDF7
SHA-512:	1B0C5F62674B53B0F4E18EA372DA78DE7C4881858117AAD29E4A0360E96FB1072F89DE99B2CDB677FA102D6B99A2D9E679BB2B39FB270F7E22F93E3F25B77B8
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\{747EC0F4-85EF-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	34924
Entropy (8bit):	1.659380233196888
Encrypted:	false
SSDEEP:	96:r+ZxQW6kBS1AQT7zgTazwr8LOr4Ld0h1gIr:r+ZxQW6kk1AQT7zgTazwr8LOr4Ld0Fr
MD5:	74F958E85AA9F538B95644752F0B0F7E
SHA1:	B6EE9F271DF8902E1CDD5D15E281074A3A285E87
SHA-256:	E3FE1EB11C0EFA4B1E6D7F57A0891A27E0286FD7BFAF1A5B8BABE05F6A73ACE8
SHA-512:	F84E1FCEA0C17C18A6F0205FDC023A7B30A70E61B754F87F5519A90B96937BB139B66E3780588AD8BA0531AB9735F898EB946D80FEB4FD3FA6E91B6E190531F2
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\{87DBBBB-85EF-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5661029043108825
Encrypted:	false
SSDEEP:	48:IwAGcprSGwpaTG4pQPGrapbSU+GQpKvG7HpRATGIpG:rkZaQl6TBSTA+TUA
MD5:	E0ACBFAE2BE97B39D14E7979CA1DA72E
SHA1:	800FF9B39389BCBE6279362B99B63C3C10E52EBA
SHA-256:	CA0BF5188BD3E5D93B6C53C5F78163F731A386C8B2E828CBF644D5BFA38AD1F2
SHA-512:	D9EC1360420DA5E0F6337AC7E5553812533BB0A34138BA1352773EFC889CF3B822FF1F9F59A03F18DFFBE74EA8FF16D60F5CACC45A5EFC0F2184F738CC7C7E7C
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	2504
Entropy (8bit):	7.599596787385088
Encrypted:	false
SSDEEP:	48:bhp9TbQhr5dME2f3FTgRKqVKLVFCDap9TbQhr5dME2f3FTgRKqVKj9l:D9TUCEs3atKn9TUCEs3atKj9l
MD5:	57C237DF1F93B8169F9918A10579196E
SHA1:	14D99D0527C37099A1038E7719EC860BC8FFCDF8
SHA-256:	2E8F039DF7C432A04543A20C914D8B489E48AB77A87F8AF53D8FC14935C84914
SHA-512:	FDC69CD6EECFBDA25194163B7D18940C0AD4BAA9FF4A5DD594F1411097E7B3C4FBFCC7716345717C05C034114B6E72B071042FB89F59CB1DEF89AA5531EE691
Malicious:	false
Reputation:	low
Preview:	(.h.t.t.p.s.:././.p.h.-.n.o.r.t.h.w.e.s.t.m.i...a.s...m.e./.f.a.v.i.c.o.n...i.c.o.j....PNG.....IHDR...0...0.....W.....sRGB.....$IDATh..Xi..Q..... KvF.(..(...EI~..P...BY..0Yj0.....2.?$Y..SLh,%d.c{.}...:...w..[.=.].....w...T.....f .3."...F.!.[.....@.Q)2.....?.....%@..28...\....9...rB.1.'..`Xy.b,..O...U%..~....:.D=.L..H.....z...c.0.t..".s..~F..N.Y..@w....&.%.c.7.....P.....F....>.D.....v`Y.....I..{..[P.4}.c.miV.....oU.*9C.s..y...W..A...Y.4...Kp..({>hhV.f.8.....oZ..Y.b.M.f.. :.....ANA.^0.A...8r[..>.?..*...)P.q.u;....'[..6..Y.u".....mK9...5...b.Bx.@....m.....v....6;.....x...B...@.]..P.r(m.....\.;..B..|...WI..v.\.W:.x..]..P.7.m.y!.M..i..i..Ya.....Z.Xl\...+.....+.K.>:...L.../....2{..x.....6.g.....q...N.cwm.....ty..%-eg=....o..&X&. 8...W....#.....t2i.....T[.x7..$Bg...,?6.....L@.m.).....z~#'F.....7@./*g.Uq.@..c..0..i...$Q...%..btl..]......M.B;'...w.....*..>..t9.....V.F..#....|=.....S.....ja3....*. ...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	203
Entropy (8bit):	5.206367642924882
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\css[1].css	
SSDEEP:	3:0SYWFFWlIYCdGgyIiRI5XwDKLRIHDfFRWdFTfqzrZqcd8WJhZB28uGUM3xuSPLBy:0IFFE0i+56ZRWHTizlpdRfnVhNin
MD5:	3F9B532C4E0BB98A6B270F466E3BB339
SHA1:	53ABE84BE49F53DEC5D83F52E384A410634E8A22
SHA-256:	D9C0984700CF3587571B497508E67E09D8B4F43917463EC7414D447B8ABD29BC
SHA-512:	1586406E815842CD18FDAAA8D424B716B003DE609D2EE9C750FE9A52C07CA34328B70149FD66DF3396E35A6E2AD77FAC2EF108115C236AFBFB1FBD8FCD23E46
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Source+Sans+Pro
Preview:	@font-face {. font-family: 'Source Sans Pro';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/sourcesanspro/v14/6xK3dSBYKcSV-LCoeQqfX1RYOo3qOK7j.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\down[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	206
Entropy (8bit):	5.091901884549508
Encrypted:	false
SSDEEP:	6:tnrLvUoDumc4slvIVQjFQCIJeGnJ60bBsFn:trLv1uC6rYBbBsN
MD5:	C652A5EF0AD8746D4DFD7A4E04EE9CB5
SHA1:	2B81B37367F2DBCD249DC7B0C1BE64091CE2396F
SHA-256:	DD1E180F1B9B88FCA4185DC8B10CE692ADAFF37E9744CE09661AAAC785FBBF55
SHA-512:	B93F90B4113DF775DC6A101AE83A8B91D825008CCA9BDA9EEBE88D06775803E20DE23BA07293FCA87B12F60711432D068947754DAC08489AD99403EDCA225F9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/down.svg
Preview:	<svg width="14" height="16" viewBox="0 0 14 16" fill="none" xmlns="http://www.w3.org/2000/svg">.<path d="M14 6.25V9L7 16L0 9L3.27934e-08 6.25L6 12.25V0L8 2.38498e-08V12.25L14 6.25Z" fill="#313131"/>.</svg>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1130
Entropy (8bit):	7.774023477258517
Encrypted:	false
SSDEEP:	24:V99gwbQM8r53dYnE+Yif6UFTKzSURuVRkOFoqN0ryNu:L9TbQhr5dME2f3FTgRKqVKc
MD5:	9E692FE534DA39B5C8F14625EB830C64
SHA1:	98CFEE2A58D900D55519E731D87AD678B5BE04FC
SHA-256:	6F18DCF9C7761928B5A69D498370F1C566EEF18BCAC4BFF21D7336AC63618D17
SHA-512:	372AA1710AFAE9A595DFE7AD131F0CA1DCC1C4A15206ECCD448CC580943D5D3367B882A1EF7A123DBECEF2CE5AA39040B2CC587125F8C12F4002E8C50B2F803
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ph-northwestmi.as.me/favicon.ico
Preview:	.PNG.....IHDR...0...0.....W.....sRGB.....$IDATh..Xi..Q..... KvF.(..(...EI~..P...BY..0Yj0.....2.?$Y..SLh,%d.c{.}...:...w..[.=.].....w...T.....f .3."...F.!.[.....@.Q)2.....?.....%@..28...\l....9...rB.1.'..`Xy.b,..O...U%..~.....:D=.L..H.....z...c.0.t..".s..~F..N.Y..@w....&.%.c.7.....P.....F....>.D.....v`Y.....I..{..[P.4}.c.miV.....oU.*9C.s..y...W..A...Y.4...Kp..({>hhV.f.8.....oZ..Y.b.M.f.. :.....ANA.^0.A...8r[..>.?..*...)P.q.u;....'[..6..Y.u".....mK9...5...b.Bx.@....m.....v....6;.....x...B...@.]..P.r(m.....\.;..B..|...WI..v.\.W:.x..]..P.7.m.y!.M..i..i..Ya.....Z.Xl\...+.....+.K.>:...L.../....2{..x.....6.g.....q...N.cwm.....ty..%-eg=....o..&X&. 8...W....#.....t2i.....T[.x7..$Bg...,?6.....L@.m.).....z~#'F.....7@./*g.Uq.@..c..0..i..$Q...%..btl..].....M.B;'...w.....*..>..t9.....V.F..#....|=.....S.....ja3....*. ...L..).M..@..L...+.....>....W..q.|...J}.xY..&K.p5...:P....y@..eB.>.z.0. ....?.?Q.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\j[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2634
Entropy (8bit):	5.432530638230725
Encrypted:	false
SSDEEP:	48:dy3k7VBaOW++NcOWDWCWM+sabC3bis9sSG2pligmnroYkG7Yu1hObxi2opaA5kiy:Q302reqTMabCmopdxnr4W4UJpy
MD5:	EB7302B99A8604E265A8F76AF27934E6
SHA1:	92D25D6C4E47C0E465D0D95EDF93AFD37B7EB068
SHA-256:	382A81D8D588D6DC4C0A4DFE8B575B61DAA2395C3428DDD766D53997418E60A3
SHA-512:	2A943D7CCE17712B59A8B04FB9E55564356082A0484D69064F08424B4E16C53357432E271ED3D48B7BEBA13D05DDAF4183461C1213E067E9AFA122D0310BBFB9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\j[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dev.visualwebsiteoptimizer.com/j.php?a=37352&u=https%3A%2F%2Fsecure.acuityscheduling.com%2Flogin.php&r=0.1522697990812168
Preview:	try{(function(){var aC=window._vwo_code;if(aC){window._vwo_j_e=window._vwo_j_e||0;if(window._vwo_j_e==1){window._vwo_mt="dupCode";clearTimeout(window._vwo_settings_timer);if(window.VWO&&window.VWO._&&window.VWO._.bIE){window._vwo_code.finish()}return}if(window._vwo_j_e==-1){window._vwo_j_e=1}}window._vwo_mt="live";try{window._vwo_tm="";var getMode=function(e){var n;if(window.name.indexOf(e)>-1){n=window.name}else{n=window.location.search.match("_vwo_m=([^&]*)");n=n&&n[1]}return n&&JSON.parse(decodeURIComponent(n))};if(window.name.indexOf("_vis_heatmap")>-1||window.name.indexOf("_vis_editor")>-1||getMode("_vwo_cc")||window.name.indexOf("_vis_preview")>-1){window._vwo_mt=window.name}else if(window._vwo_tm.length){window._vwo_mt=window._vwo_tm}else if(location.href.indexOf("_vis_opt_preview_combination")!==-1&&location.href.indexOf("_vis_test_id")!==-1){window._vwo_mt="sharedPreview"}if(window._vwo_mt!=="live"){if(!getMode("_vwo_cc")){_vwo_code.load('https://dev.visualwebsiteoptimizer.com

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	85578
Entropy (8bit):	5.366055229017455
Encrypted:	false
SSDEEP:	1536:EYE1JVoiB9JqZdXXe2pD3PgoIiulrUndZ6a4tfOR7WpfWBZ2BJda4w9W3qG9a986:v4J+OlfOhWppCW6G9a98Hr2
MD5:	2F6B11A7E914718E0290410E85366FE9
SHA1:	69BB69E25CA7D5EF0935317584E6153F3FD9A88C
SHA-256:	05B85D96F41FFF14D8F608DAD03AB71E2C1017C2DA0914D7C59291BAD7A54F8E
SHA-512:	0D40BCCAA59FEDECF7243D63B33C42592541D0330FEFC78EC81A4C6B9689922D5B211011CA4BE23AE22621CCE4C658F52A1552C92D7AC3615241EB640F8514B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js
Preview:	/*! jQuery v2.2.4 | (c) jQuery Foundation | jquery.org/license */!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="2.2.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,function(b,c){return a.call

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\notice[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	16600
Entropy (8bit):	5.259128738228789
Encrypted:	false
SSDEEP:	384:PBuFyxyviZvb657k9T6sEGPIM/lyXq43GNk:PZYviZG5mQzXq43D
MD5:	C2CCE6DF0689A43C28AE12A053677CBC
SHA1:	AA32B9431DA83FAE5F0AE7CA1CB2D04E2FBA436F
SHA-256:	C29EB102A3BB555F982C31448D88CE74F58BC987E879A06328D15206D6FCEE24
SHA-512:	643140D31816823F04944F67A18D3487380BA02E567971FA4DF452D304A9E9FF51B19710C0A0E8941EE6DEE7F7E4BE71FDA32E137AD0657D411D1E22ED849498
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://consent.trustarc.com/notice?domain=squarespace.com&country=ch&js=nj2&c=teconsent¬iceType=bb&text=true&pn=2>m=1&pcookie
Preview:	truste.bn.round=function(b,a){return Number(Math.round(b+"e"+a)+"e-"+a)};truste.bn.getDefaultStyleProperty=function(a,b){var c=document.createElement(b);.document.body.appendChild(c);var d=window.getComputedStyle(c,null)[a];c.parentNode.removeChild(c);return d.};truste.bn.getDisplayProperty=function(b){var a=window.getComputedStyle(b,null).display;return(a=="none")?truste.bn.getDefaultStyleProperty("display",b.nodeName):a.};truste.bn.show=function(c){if(!c){return}var b=truste.bn.getDisplayProperty(c);if(typeof requestAnimationFrame!=="undefined"){c.style.opacity=0;.c.style.display=b;(function a(d){var e=truste.bn.round(parseFloat(d.style.opacity),2);if((e=e+0.1)<=1){d.style.opacity=e;.requestAnimationFrame(function(){a(d)})}})(c)}else{c.style.display=b}};truste.bn.hide=function(b){if(!b){return.}if(typeof requestAnimationFrame!=="undefined"){(function a(c){var d=truste.bn.round(parseFloat(c.style.opacity||1),2);.d=d-0.1;c.style.opacity=d;if(d<=0){c.style.display="none"}else{requestAni

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\right[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	377
Entropy (8bit):	4.72214112136362
Encrypted:	false
SSDEEP:	6:tnrCtzURDumc4slvI7Uj5jgSU7KMrluLULhzIVESVtT5Q6NsPT23XocqIjVdVDNh:trUzSuC7NSUPAo9yESVh5Q6NsIBJjXjF
MD5:	61761C08EF4C600B96F5F99D3BE63476
SHA1:	175EA4D34267AB2AF35AD07AB72B13EDF2A8423B
SHA-256:	3ACD6635066A6BDC6088EA0251B78E76A4D76AD40D18C8F6BE6DF38FF4075D82

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\right[1].svg	
SHA-512:	0AF3D988B0C7FCEB8171BF581DC41EA035B45BD58CC5C3F87D6D20B741CA84584F189F9CB5FAFB8815708B76B21B5967542CB4CF063732E8B119EE54EF61918
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/right.svg
Preview:	<svg width="15" height="12" viewBox="0 0 15 12" fill="none" xmlns="http://www.w3.org/2000/svg">.<path d="M0.909191 7.176H11.0972C10.7552 7.572 10.0712 8.166 9.29719 8.94L6.30919 12H9.04519C10.4672 10.578 13.0772 7.698 14.5892 6.168C13.0772 4.656 10.4492 1.812 9.04519 0.354H6.30919L9.29719 3.414C10.0892 4.224 10.7372 4.818 11.0972 5.196H0.909191V7.176Z" fill="black"/>.</svg>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\site-gavins-goodies[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	9473
Entropy (8bit):	3.8997297908439794
Encrypted:	false
SSDEEP:	192:XGrZK6k1LWYUf+aKppeja3VHlWDKsx4rUDtuJACjzaVA5RLiV1ujiFY:UY6kdLJ7VHlW76rauJcA5RO7VFY
MD5:	967DE272FF3C383B76956BD95A71731C
SHA1:	72F9AE25750C90D59646C47CC701BE57B0ADC1F7
SHA-256:	1738513C6194F541278AB00F38AB102CF7858EAD8A61EBBC1CDAEE5ED2C439A2
SHA-512:	03ED04377B8594F707E9C6DD0797BF9D8098DB6CF7ED8DF8668CAA16275EECF4AC658A0FA1103F7F530FEAA539793EB3F9C66C94BB4AC811ECEA7FFC67B8C/D1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/site-gavins-goodies.svg
Preview:	<svg width="475" height="340" xmlns="http://www.w3.org/2000/svg"><g fill-rule="nonzero" fill="none"><path fill="#CAC7BB" d="M0 0h475v340H0z"/><g fill="#FFF"><path d="M114.079 209.265c0-1.358.235-2.557.706-3.6.471-1.043 1.1-1.91 1.886-2.606a7.96 7.96 0 0 1 2.568-1.516 8.448 8.448 0 0 1 2.898-.522c.974 0 1.94.175 2.899.522.954.345 1.84.859 2.614 1.516.755.695 1.367 1.564 1.838 2.606.472 1.043.708 2.242.708 3.6v1.707h-4.807v-1.706c0-1.169-.322-2.03-.966-2.582-.645-.553-1.407-.832.285-.83-.88 0-1.643.277-2.286.83-.644.553-.966 1.414-.966 2.581v17.816c0 1.168.322 2.03.966 2.582.643.552 1.406.829 2.285.829.88 0 1.641-.276 2.285-.829.645-.552.967-1.414.967-2.582v-6.349h-3.817v-4.264h8.624v10.613c0 1.421-.236 2.638-.708 3.649-.47 1.01-1.083 1.847-1.837 2.51a8.073 8.073 0 0 1-2.615 1.565 8.46 8.46 0 0 1-2.9.52 8.448 8.448 0 0 1-2.897-.521 7.554 7.554 0 0 1-2.569-1.564c-.785-.663-1.414-1.5-1.885-2.51-.47-1.011-.706-2.227-.706-3.65v-17.815zm20.358 25.776v-33.735h4.807v28.902h9.52v4.833h-14.327zm

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\site-llama-ste[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	10646
Entropy (8bit):	3.851069005886839
Encrypted:	false
SSDEEP:	192:Fh7v7ADHMBoervMfvGgApy0WNUHz13q5BAUqVkgkcer/:FhADsV+vhAp4UTY8Jter/
MD5:	C84F264FF4C59F5EF51A79214ECAC5E0
SHA1:	1A847691E2142BB2C9CAAC9C00CD29FFF3114AC5
SHA-256:	8D4C6970718173FF794872D46DFE00836D05F46BAF05F24518BA8E04DB3BDD9B
SHA-512:	81E7E18DCE5421530CA2115B059B87C51149342043374F6950676FC95B3261318728D9570B79273DED2171C8A7374DD65BD5DB80B94AC0C91AA6EAF2D1605EBF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/site-llama-ste.svg
Preview:	<svg width="475" height="340" xmlns="http://www.w3.org/2000/svg"><g fill-rule="nonzero" fill="none"><path fill="#C1CED4" d="M0 0h475v340H0z"/><g fill="#FFF"><path d="M141.702 237.34v-21.334c0-.92.475-1.43 1.39-1.43h1.56c.917 0 1.39.51 1.39 1.43v18.982h8.989c.95 0 1.425.478 1.425 1.398v.954c0 .954-.475 1.431-1.425 1.431h-11.938c-.916 0-1.391-.477-1.391-1.43zm19.79 0v-21.334c0-.92.475-1.43 1.39-1.43h1.56c.917 0 1.39.51 1.39 1.43v18.982h8.989c.95 0 1.425.478 1.425 1.398v.954c0 .954-.475 1.431-1.425 1.431h-11.939c-.915 0-1.39-.477-1.39-1.43zm17.552-.205l7.53-21.401c.27-.784.78-1.159 1.593-1.159h2.171c.814 0 1.357.375 1.594 1.159l7.53 21.402c.338.988-.103 1.635-1.153 1.635h-1.561c-.813 0-1.357-.375-1.594-1.158l-1.696-5.045h-8.445l-1.662 5.01c-.238.818-.78 1.194-1.594 1.194h-1.56c-1.051 0-1.492-.648-1.153-1.637zm7.055-8.143h6.274l-2.136-6.477c-.408-1.364-.95-3.749-.95-3.749h-.068s-.543 2.386-.95 3.75l-2.17 6.475zm18.026 8.314l1.73-21.368c.101-.885.576-1.364 1.459-1.364h2.135c.815 0 1.323.376

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\site-whiskey-business[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	20454
Entropy (8bit):	3.7437039764100395
Encrypted:	false
SSDEEP:	384:DPZOaNrXQZOaZZOaKt2vUtZA5ROYd8qtpwmtLKC4OeS36sADaD8i48D:dOyrWOyORfID9Nt6ILKCqtND/f8D
MD5:	A2C6897AEAFF14C0A3472E426BE26AEE
SHA1:	3F077CA69B9CF24896B68857E5D94B00BD21FA1B
SHA-256:	907745ED0C8F63B057D22233E40DF394FA09FC67E542B414050EDE2836EEF01B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\site-whiskey-business[1].svg	
SHA-512:	7636AEEB8857DB588D24C28E8A933ED407B3CB147C5EE15AD0C7D49A2ECC97C1D6E0A142E1DEB2BB7BD45E337905E577BFBC40020905CECE115C0D0BAAF8345B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/site-whiskey-business.svg
Preview:	<svg width="475" height="340" xmlns="http://www.w3.org/2000/svg"><g fill="none" fill-rule="evenodd"><path fill="#BBCABE" d="M0 0h475v340H0z"/><g fill="#FFF" fill-rule="nonzero"><path d="M212.339 190.24a.672.672 0 0 0-.12-.42c-.08-.104-.232-.156-.456-.156v-.288h8.256c.768 0 1.42.084 1.956.252.536.168.972.4 1.308.696.336.296.58.64.732 1.032.152.392.228.82.228 1.284 0 .624-.132 1.164-.396 1.62-.264.456-.732.772-1.404.948v.048c.688.16 1.216.516 1.584 1.068.368.552.552 1.22.552 2.004 0 1.168-.368 2.072-1.104 2.712-.736.64-1.944.96-3.624.96h-8.088v-.288c.224 0 .376-.052.456-.156a.672.672 0 0 0 .12-.42V190.24zm7.512 4.176c.912 0 1.544-.136 1.896-.408.352-.272.528-.688.528-1.248s-.176-.976-.528-1.248c-.352-.272-.984-.408-1.896-.408h-5.496v3.312h5.496zm.528 5.856c.768 0 1.348-.176 1.74-.528.392-.352.588-.864.588-1.536s-.196-1.184-.588-1.536c-.392-.352-.972-.528-1.74-.528h-6.024v4.128h6.024zm8.298-10.032a.672.672 0 0 0-.12-.42c-.08-.104-.232-.156-.456-.156v-.288h3.168v.288c-.224 0-.376.052-.456.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\v1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	71284
Entropy (8bit):	5.3102678375920425
Encrypted:	false
SSDEEP:	1536:fQIyrvmpBK3npoJcnfqqBpK3QIBKjialNUXF/9H7CZClyZwBAcD5B/DW6sZx:YxupBK3p8wpCQIBK2aXiF/9WZCWrj
MD5:	18B3B01DE8F5C3837A24BA2F60983237
SHA1:	2DC18EDAB744CB2095CA4067E84CCD68BAE5D7DA
SHA-256:	C24D4269E2737F585E331C7D7F111AA2E5945BCF4A0600DDBC9B52F20375B60E
SHA-512:	B1A7982902496EAAFB648478C201003BCA29EAB91F47795D282EF5C415B755AEF25F4BBE2386897129EE1FD15BABE07B7B6CE3D4C3D093779EDF84E6C35B9341
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://consent.trustarc.com/asset/notice.js/v/v1.7-226
Preview:	function _truste_eu(){function v(){var h=truste.eu.bindMap;h.feat.isConsentRetrieved=h.feat.crossDomain?h.feat.isConsentRetrieved:!0;if(!v.done&&h.feat.isConsentRetrieved){v.done=!0;truste.eu.ccpa.initialize();truste.eu.dnt();var l=function(){var a=truste.eu.bindMap;if(a.feat.consentResolution){var b=truste.util.readCookie(truste.eu.COOKIE_GDPR_PREF_NAME,!0);if(b&&(b=b.split(":"),!RegExp(a.behavior+"."+a.behaviorManager).test(b[2])&&(/(,us|none)/i.test(b[2])||"eu"==a.behaviorManager&&/implied.eu/i.test(b[2])))return!0}return!1},.a=function(){var a=(new Date).getTime(),b=truste.util.readCookie(truste.eu.COOKIE_REPOP,!0),c=truste.eu.bindMap.popTime;return c&&c!=b&&a>=c}();a&&(h.feat.dropPopCookie=!0);h.feat.isDNTOptoutEvent?h.feat.dntShowUI&&"expressed"==h.behavior&&(truste.eu.clickListener(truste.eu.noticeLP.pn,!0),truste.eu.msg.log("consent",h,h.messageBaseUrl)):null!=truste.util.getIntValue(h.prefCookie)?("expressed"==h.behavior&&(a||l())&&(h.feat.isRepopEvent=!0,h.feat.isReconsentEv

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\fontawesome-webfont[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), FontAwesome family
Category:	downloaded
Size (bytes):	60767
Entropy (8bit):	7.983356702664012
Encrypted:	false
SSDEEP:	1536:CIRF2F4AF5tUe8gNkngPj3XxBe1zE97WCVksAb:CIRo4AFvUtg3r3QzatmsC
MD5:	F7C2B4B747B1A225EB8DEE034134A1B0
SHA1:	3E63FC9B3DE4580F1F3BEC0631436F755B80F167
SHA-256:	CBB644D0EE730EA57DD5FBAE35EF5BA4A41D57A254A6B1215DE5C9FF8A321C2D
SHA-512:	F8B32EEC082C86A295931F39A38C1B638254F4D298CE97DE8D4C80504340CB922D18770C445A19854AA6BCA27E12E234957C7D17C78361FA19CEEA1DB7E5491
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/responsive/css/fonts/fontawesome-webfont.eot
Preview:	_...y.....LP.....P.....F.o.n.t.A.w.e.s.o.m.e.....R.e.g.u.l.a.r...$.V.e.r.s.i.o.n. .4...3...0. .2.0.1.5...&.F.o.n.t.A.w.e.s.o.m.e. .R.e.g.u.l.a.r..... BSGP.....T..q..u..*.....Y.D.M.F..x...>.....)Y.....h..D....pj....f.i..).U.'.&a..;`.*../.....V.B.....OV..r.n.:..{$2D....:.&...m..d ..CeH.\./o.....U.M....X.`?...?.A...C...@..'.(g~.....%(.Jl.&zw....W#.mw".].At....k.....p...E....[..=.gM.....go..W.R.q..`{.ZwUF.....o ..D.p)A8....$..M.#.>..?..... d.No2..L.....<.t...B..T..a....<...`.....e.SO....cl[.p..E1R*.fMd....>..2V.....z7..&.+.....f.&#.V.(8....aR.....x.Z\R.e..$.Vw.....K....gs.....*.... ..dI.....6.....)...rj..:Z."1.'...<....'.Q/...8.).B..5..tgk.AM.)...|~...."...2....+h..(.&.c..sw...(....h.Dg.k...w.zm%.f..../5.%....}...k..... ..@...[#.D)..J<..?YAT.....o.s%..Z...G).5....#R'...#...)...+R.....Z.z...+._....K&%'5....(b....Y..i_.....|B.>U.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\gtm[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	155272
Entropy (8bit):	5.5273109295388005
Encrypted:	false
SSDEEP:	3072:SeRuVFWFWhZzL640Gjs+ftQH20ubSA7vyevM9IW8:SeRPIz3NX2eLyeEo
MD5:	5E83CFF4FA4D8BD57E25BCB2C9B965AA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\gtm[1].js	
SHA1:	5C01221514AE7A739486A6AB22BF167A3397B009
SHA-256:	5594F494AD8B37E8323A37FBFC4E84FC4B2F482451B79FD56D355ECAFCB9DE75
SHA-512:	98E9DD083CD7F228A29EB165A3C71D810DC379FE0F8163DA134F72277B42465D21D511C37C64ED2080572E2A8DD4A5749ABFE4FF2B2E33CE7DD859C2BB6A41C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googletagmanager.com/gtm.js?id=GTM-5G77WWT
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"40",. . "macros":[{. "function":"__e". },{. "function":"__k",. " vtp_decodeCookie":false,. "vtp_name":"cmapi_cookie_privacy". },{. "function":"__k",. "vtp_decodeCookie":false,. "vtp_name":"notice_behavior". },{. "function":"__gas",. "vtp_cookieDomain":"auto",. "vtp_doubleClick":false,. "vtp_setTrackerName":false,. "vtp_useDebugVersion":false,. "vtp_useHashAutoLink":false,. "vtp_decorateFormsAutoLink":false,. "vtp_enableLinkId":false,. "vtp_enableEcommerce":false,. "vtp_trackingId":"UA-1071942-1",. " vtp_enableRecaptchaOption":false,. "vtp_enableUaRlsa":false,. "vtp_enableUseInternalVersion":false,. "vtp_enableGA4Schema":false. },{. "function":"__u",. "vtp_component":"URL",. "vtp_enableMultiQueryKeys":false,. "vtp_enableIgnoreEmptyQueryParam":false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\j[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2697
Entropy (8bit):	5.446875647274145
Encrypted:	false
SSDEEP:	48:dy3k7VBaOW++NcOWDWCWM+sabC3bis9sSmwJpIigmnroYkG7Yu1hObxi2opaAXqk:Q302reqTMabCmxwJpdxnr4W4Unqpy
MD5:	880648A4CE74C0E2E6AB959E2988EDB9
SHA1:	2478D7AA783A6560B4AF08EDD960A1B079CB696E
SHA-256:	A8C743F1D11B38C0C307D275257BDF4C08275DEE3214540153B16FA60224E458
SHA-512:	00F0D3C33C6FAFB1F6C26B4DACC5DFDBE6DAE1765FE4377D89D6CED8066E9E2B0C0298E5D9D280D79491241616198CA3CA8A326526459B991705D8A3700EB7F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dev.visualwebsiteoptimizer.com/j.php?a=37352&u=https%3A%2F%2Fwww.acuityscheduling.com%2F%3Futm_campaign%3Dacuity%26utm_medium%3Dreferral%26utm_source%3Dscheduling&r=0.022163230142868 86
Preview:	try{(function(){var aC=window._vwo_code;if(aC){window._vwo_j_e=window._vwo_j_e||0;if(window._vwo_j_e==1){window._vwo_mt="dupCode";clearTimeout(window._vwo_settings_timer);if(window.VWO&&window.VWO._&&window.VWO._.bIE){window._vwo_code.finish()}return}if(window._vwo_j_e==-1){window._vwo_j_e=1}}window._vwo_mt="live";try{window._vwo_tm="";var getMode=function(e){var n;if(window.name.indexOf(e)>-1){n=window.name}else{n=window.location.search.match("_vwo_m=([^&]*)");n=n&&n[1]}return n&&JSON.parse(decodeURIComponent(n))};if(window.name.indexOf("_vis_heatmap")>-1||window.name.indexOf("_vis_editor")>-1||getMode("_vwo_cc")||window.name.indexOf("_vis_preview")>-1){window._vwo_mt=window.name}else if(window._vwo_tm.length){window._vwo_mt=window._vwo_tm}else if(location.href.indexOf("_vis_opt_preview_combination")!==-1&&location.href.indexOf("_vis_test_id")!==-1){window._vwo_mt="sharedPreview"}if(window._vwo_mt!=="live"){if(!getMode("_vwo_cc")){_vwo_code.load('https://dev.visualwebsiteoptimizer.com

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\left[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	376
Entropy (8bit):	4.716809723213467
Encrypted:	false
SSDEEP:	6:tnrCtzURDumc4slvIHVcwRK6bbtTe9ngLpqpIxMexCVXAp8X9SbPRMSXeoD52:trUzSuCH1K6bb7VqpUtx4wStc1X0
MD5:	B2FB2DC4CA6A3F46D4A2F14DAE2F05A7
SHA1:	AF9F2F76D11D859AC5256B89E1049C2F368F176F
SHA-256:	78E4DB1A311F6435762EDDC8A3B5A31D8B362995CC794385B5243A555CED0E9F
SHA-512:	BD5F4DCA221BC3809FC4BE5F976CA7493D79A9AFEE5F3A31D3D8DE7F3CE4D6E02DCA42ED50E90115D67AE5AA3D35D4B39E60DA6E8505F2814E497A9094C3139
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/left.svg
Preview:	<svg width="15" height="12" viewBox="0 0 15 12" fill="none" xmlns="http://www.w3.org/2000/svg">.<path d="M14.6597 7.176V5.196H4.47172C4.83172 4.818 5.47972 4.224 6.27172 3.414L9.25972 0.354H6.52372C5.11972 1.812 2.49172 4.656 0.979721 6.168C2.49172 7.698 5.10172 10.578 6.52372 12H9.25972L6.27172 8.94C5.49772 8.166 4.81372 7.572 4.47172 7.176H14.6597Z" fill="black"/>.</svg>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\login[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	32934
Entropy (8bit):	5.454768098404652
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\login[1].htm	
SSDEEP:	768:wLtvyk1Tsk0s/MD1iuyj1U4lWeX2oTzGJtGnXlc5EHvFuk:wLt9G4ke/PGJYnXm5EHvFuk
MD5:	5C2CCC4F4A163DC3F5F6E09D1D60F02A
SHA1:	B6AA1FC06DC03AEB1C4445B2E7922414747B4EE3
SHA-256:	87D2587AC75E9DB18E7652E162901686A025F502E2EEF3025E95785E4919F612
SHA-512:	6A3E4866CF813DDB0579BBCB6E55037A75B5C88D4023E7C13822205B656F83C87E72032AA5ECF363ABF06E6D3A206B837CDA950B549C0E836539C91819A0383A
Malicious:	false
Reputation:	low
Preview:	.<!DOCTYPE html>.<html lang="en">.<head>..<script...src="//consent.trustarc.com/notice?domain=squarespace.com&c=teconsent&js=nj&noticeType=bb&text=true&pn=2&gtm=1&pcookie"...crossorigin="">..>..</script>.. Google Tag Manager -->.<script nonce="a79c61d40faeeec0cf0f11f23027682453e052a9c1430d0fac30e89e43da9d3b4f49594a72f360179f36fbdbdf21c928ef33cab92638b8ec2463d4e611c1d08b">..(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':.new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],.j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src=.'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);.})(window,document,'script','dataLayer','GTM-5G77WWT');.</script>. End Google Tag Manager -->..... Start Visual Website Optimizer Asynchronous Code -->...<script nonce="a79c61d40faeeec0cf0f11f23027682453e052a9c1430d0fac30e89e43da9d3b4f49594a72f360179f36fbdbdf21c928ef33cab92638b8ec2463d4e611c1d08b">.....var _vwo_code = (funct

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\login[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	4410
Entropy (8bit):	5.062051302022341
Encrypted:	false
SSDEEP:	96:oHCOik5FxawidKkJ0tlz8FNs/b+UhWmUidlURbbdr/9bmVHdhB:oRSwhklbs/bAT/W9H
MD5:	A7A2CD799B837E2A6B4566B4D3271EEB
SHA1:	5C48CA0F2C1B5ED670B81D431400FF12ABA75B1F
SHA-256:	9BB24DADD62FC5B3A76C7160A8ADA363AF44545CBA1DA2CA03637C7E87E02D52
SHA-512:	3EE3844E2A4FF7594A33848FD846493B4664FCC21E1B0F0FE54007280CB8A10EA509C90201653509FAE4D1E1BD4F28A0BDAAE458049EC34B7319BCDE3CFF817
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secure.acuityscheduling.com/responsive/js/login.js?v=c1a593
Preview:	(function() {..var usernameField = $('#username');..var passwordContainer = $('#password-container');..var passwordField = $('#password');..var nextButton = $('#next-button');..var usernameError = $('#username-error');..var form = $('#login-form');..var chooseLogin = $('#choose-login');..var squarespaceContinue = $('#squarespace-continue');..var acuityContinue = $('#acuity-continue');..var wasSubmitted = false;..var forgotPassword = $('.forgot-password');..var baseUrl = $('#oauth-data').data('base-url') || '/';..var squarespaceUrl = $('#oauth-data').data('squarespace-url');..var loginButtonText = $('#oauth-data').data('login-button-text');.../// <sl:translate>..var loadingStr = 'Loading...';..var nextStr = 'Next';../// </sl:translate>...if (usernameField.val()) {...nextButton.prop('disabled', false);..}...if (...typeof localStorage !== 'undefined' &&...localStorage.getItem('acuity-oauth') === usernameField.value..) {...showPasswordField();..}...$('#username').on('input', function() {...h

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\logo-square[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3894
Entropy (8bit):	3.9675651706222856
Encrypted:	false
SSDEEP:	96:OO4DAIK1L8nKfJwEGrmaQ5fcuPawBQIdBJjldSviG:O/DAR1wnKfJwEsm39nhlnJhkviG
MD5:	179C1C854F83E042B47110E667FF3530
SHA1:	254F74B9101C2C8AAF33E6E95EEABED8C52CABC0
SHA-256:	AECE993E18F1BB13FB8509DF3CB2DD082EB97BEFF201EBFD71C27817F6891AAC
SHA-512:	C8E08650F72D8BB4FD7B558EE7FA15E73E18F3867E5E3C38859F3F3C51192D2FD0C9CB44E7F24B04906EF3534691B3D7B8943B71E341942BF003EFBF59CF16D8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/logo-square.svg
Preview:	<svg width="112" height="28" viewBox="0 0 112 28" fill="none" xmlns="http://www.w3.org/2000/svg">.<path fill-rule="evenodd" clip-rule="evenodd" d="M22.7994 0.106241H4.67453C2.18275 0.106241 0.143311 2.14877 0.143311 4.64518V22.794C0.143311 25.2889 2.18275 27.3306 4.67453 27.3306H22.7994C25.2904 27.3306 27.3307 25.2889 27.3307 22.794V4.64441C27.3307 2.14877 25.2904 0.105469 22.7994 0.105469V0.106241ZM22.3872 20.9391C22.386 21.321 22.2336 21.6869 21.9634 21.9568C21.6932 22.2267 21.3272 22.3787 20.9453 22.3795H6.52716C6.14532 22.3787 5.77934 22.2267 5.50926 21.9567C5.23918 21.6868 5.08699 21.3205.08597 20.9391V6.50013C5.08597 5.70659 5.73439 5.05662 6.52716 5.05662H20.9445C21.7373 5.05662 22.3864 5.70659 22.3864 6.50013V20.9391H22.3872ZM17.4453 16.6055C17.4453 17.0609 17.0748 17.4314 16.6225 17.4314H10.8554C10.6368 17.4306 10.4276 17.3432 10.2733 17.1884C10.1191 17.0336 10.0325 16.824 10.0325 16.6055V10.8314C10.0325 10.3775 10.4015 10.007 10.8554 10.007H16.6217C17.0748 10.007 17.4453 10

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\logo-zapier[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	8002
Entropy (8bit):	3.9053149307405612
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\logo-zapier[1].svg	
SSDEEP:	192:AscH6qr99CD6BiXW4iC7EXJtu22iaAk6G5/:A/62DC7Fm1G5/
MD5:	0273D2CBB113C47E2EE75BFB52DE3678
SHA1:	1402893A87EC3583C2FC368FC1A49A59D90005BE
SHA-256:	3E7821078D82CE435B640CBF4D6848486BECDE92AB1A6F21CBDE3ADEC59A8AF6
SHA-512:	F820A2BBBCA4DF86A8EDDD527ADE6B9F00102244FE0E19787E3A5BEAAF827DD14BF03FF116E1E0AB69DDE7E517FD9681B8D0F338A866C6D8689F3E469B00D9EB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/logo-zapier.svg
Preview:	<svg width="78" height="38" viewBox="0 0 78 38" fill="none" xmlns="http://www.w3.org/2000/svg">.<g clip-path="url(#clip0)">.<path d="M46.9546 16.6239H45.028C44.9847 16.4382 44.955 16.2493 44.9391 16.059C44.8998 15.6422 44.8998 15.2224 44.9391 14.8055C44.9592 14.5929 44.9885 14.4041 45.028 14.2406H49.8288V29.9151C49.5883 29.9583 49.3458 29.9887 49.1023 30.0064C48.8612 30.0254 48.6185 30.0349 48.3759 30.0365C48.144 30.0349 47.9122 30.0246 47.6803 30.0064C47.437 29.9885 47.1948 29.9578 46.9546 29.9144V16.6231V16.6239ZM63.6671 20.5653C63.6671 19.9949 63.5929 19.4507 63.4453 18.931C63.3105 18.4407 63.0894 17.9798 62.793 17.5712C62.5006 17.1797 62.1257 16.8613 61.6964 16.6398C61.252 16.4049 60.7234 16.2883 60.1113 16.2883C58.9057 16.2883 57.9821 16.6652 57.3407 17.4189C56.6985 18.1726 56.3082 19.2214 56.1699 20.5653H63.6671ZM56.1397 22.8264C56.1799 24.5377 56.6096 25.7904 57.4296 26.5846C58.2488 27.378 59.459 27.7762 61.0596 27.7762C62.4615 27.7762 63.7954 27.5216 65.0597 27.0122C65.2174 27.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\logo_inverse[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	11736
Entropy (8bit):	4.163308901694307
Encrypted:	false
SSDEEP:	192:7dHJXtlEM7yqgvrCWPYTanEild5wtcuSnDETLEb4KJgOIWztUhFe1naIxOxGr1Yg:KD8iJwulDEUb4EiAtEFokorkESC
MD5:	8EF5F99EFA844294DF0A843751BE93BB
SHA1:	75378B5AE9FB1E2F869ECDE512966867E20B4C1C
SHA-256:	06A32F58B9A529E08BFCE28EC42D92E1BB59CFFA6AE8F870D38270D656A56FA8
SHA-512:	BA043CA9A75731143F889E8DA9A211FA71F77BA7D150E126325F6A3EE9B972D8738ECB67D9BE174E4A279E2928CC8421B0488125BD3EA5FBB11816222C419315
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secure.acuityscheduling.com/img/marketing/squarespace/logo_inverse.svg
Preview:	<svg width="230" height="33" viewBox="0 0 230 33" fill="none" xmlns="http://www.w3.org/2000/svg">.<path d="M0.175995 31.3941H1.46299L2.255 29.1391H5.676L6.46799 31.3941H7.832V31.0091L5.06 23.4961H2.981L0.175995 31.0091V31.3941ZM3.124 26.7081C3.498 25.6521 3.652 25.1901 3.828 24.6951H4.1689C4.32299 25.1681 4.51 25.7291 4.851 26.7081L5.27999 27.9621H2.673L3.124 26.7081Z" fill="black"/>.<path d="M12.4567 29.2711C12.7097 30.8111 13.8647 31.5701 15.4927 31.5701C17.2417 31.5701 18.4737 30.5911 18.4737 29.1171C18.4737 27.7421 17.6047 27.3021 16.1857 26.8621L15.6247 26.6861C14.7227 26.4001 14.1727 26.1911 14.1727 25.5311C14.1727 24.9481 14.6567 24.5301 15.4597 24.5301C16.3177 24.5301 16.7907 24.9151 16.9557 25.5751L18.2757 25.4651C18.1107 24.1781 17.1207 23.3421 15.5037 23.3421C13.7767 23.3421 12.6987 24.2881 12.6987 25.6081C12.6987 26.8621 13.5567 27.5001 14.9647 27.8961L15.5587 28.0611C16.4717 28.3141 17.0327 28.5011 17.0327 29.2161C17.0327 29.9311 16.4827 30.4151 15.5367 30.4151C14.5797 30

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\notice[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	11752
Entropy (8bit):	5.3690327467406025
Encrypted:	false
SSDEEP:	192:+zIDjdV75NWzZC4fL9GS6uFvfpdOk92z1bvFdvkbjTl0yLsYYxWzKDw:JDjLYZC4fJGS6s92z3dvfyLXzf
MD5:	BD2BAEA3F8E97A63FC9D0D7EB325FA2F
SHA1:	E51C62E2303B99ACDB2A2060A721692169C5ACE3
SHA-256:	8CF55C8FF49C1F8CC211CDE39E94ACFF3BDED38B8699D9987041558AEB461065
SHA-512:	83C55F39930E92DB33B9156D4D0836C361F10C253493F015A1088E4D657D36A56A51FFCFFA52C44F1BCAEFAEE6C40E3C291378F1FA0A443D61EA4426E740D48
Malicious:	false
Reputation:	low
Preview:	(new Image(1,1)).src=("https://consent.trustarc.com/log".replace("http:","https:"))+"?domain=squarespace.com&country=ch&state=&behavior=implied&c="+(((1+Math.random())*65536)|0).toString(16).substring(1);.var truste=window.truste||{};truste.bn||(truste.bn={});truste.eu||(truste.eu={});truste.util||(truste.util={});.truste.util.error=function(h,d,g){g=g||{};var f=d&&d.toString()||"",c=g.caller||"";if(d&&d.stack){f+="\n"+d.stack.match(/(@|at)[^\n\r\t]*/)[0]+"\n"+d.stack.match(/(@|at)[^\n\r\t]*$/)[0].}truste.util.trace(h,f,g);if(truste.util.debug||!d&&!h){return}var a={apigwlambdaUrl:"https://api-js-log.trustarc.com/error",enableJsLog:false};.if(a.enableJsLog){delete g.caller;delete g.mod;delete g.domain;delete g.authority;g.msg=h;var e=new (self.XMLHttpRequest||self.XDomainRequest||self.ActiveXObject)("MSXML2.XMLHTTP.3.0");.e.open("POST",a.apigwlambdaUrl,true);e.setRequestHeader&&e.setRequestHeader("Content-type","application/json");.e.send(truste.util.getJSON({info:truste.util.getJSON(g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\notice[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	11752
Entropy (8bit):	5.380676606415507

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\notice[2].js	
Encrypted:	false
SSDEEP:	192:+zIDjdV75NWzZC4fL9E4jNaS6uFvfpdOk92z1bvFdvkbjTl0yLsYYxWzKDw:JDjLYZC4fJE4jNaS6s92z3dvfyLXzf
MD5:	1FC97801D1B704C16923C252A3E8298A
SHA1:	6A7043DA52B136F09C3D6DE3615A1EA6FE3E6CD0
SHA-256:	FCEF61410B3F39D0A648D42CA2187DF372B519208B0B7225EEFFD9B04672BA8C
SHA-512:	310B57A7192AECB465E06BE24B6877C900AAB683DE729A60CAD5DA962CBFAB5F228DC91AC82BA566826FC16C0AC5D0570049D0C17A6987E829EA0DAC636454 56
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://consent.trustarc.com/notice?domain=squarespace.com&c=teconsent&js=nj¬iceType=bb&text=true&pn=2>m=1&pcookie
Preview:	(new Image(1,1)).src=("https://consent.trustarc.com/log".replace("http:","https:"))+"?domain=squarespace.com&country=ch&state=&behavior=implied&c="+(((1+Math.ra ndom())*65536)|0).toString(16).substring(1);.var truste=window.truste||{};truste.bn||(truste.bn={});truste.eu||(truste.eu={});truste.util||(truste.util={});.truste.util.error=funct ion(h,d,g){g=g||{};var f=d&&d.toString()||"",c=g.caller||"";if(d&&d.stack){f+="\n"+d.stack.match(/(@|at)[^\n\r\t]*/)[0]+"\n"+d.stack.match(/(@|at)[^\n\r\t]*$/)[0].}truste.util.trac e(h,f,g);if(truste.util.debug||d&&!h){return}var a={apigwlambdaUrl:"https://api-js-log.trustarc.com/error",enableJsLog:false};.if(a.enableJsLog){delete g.caller;delete g .mod;delete g.domain;delete g.authority;g.msg=h;var e=new (self.XMLHttpRequest||self.XDomainRequest||self.ActiveXObject)("MSXML2.XMLHTTP.3.0");.e.open ("POST",a.apigwlambdaUrl,true);e.setRequestHeader&&e.setRequestHeader("Content-type","application/json");.e.send(truste.util.getJSON({info:truste.util.getJSON(g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\schedule[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	150297
Entropy (8bit):	5.189908264763574
Encrypted:	false
SSDEEP:	1536:8xI1hRdHyut95Uz7SM+mdrJDRwk9MzLizs:8sHlX5e7SM+mdrlRwkw
MD5:	6369014A6126DAA5CC57F4BDC095C9E3
SHA1:	368B464A9693A27093861C9CBE7EAD9CB664DBF2
SHA-256:	9C76B3DB094FCFABBFD83AC495B6AD96B862222BB5E6DA0CE3B375601C3A79A1
SHA-512:	52D3E89D14A4884381664A96341B1D4FF389AA80863D4947CA9FEC6638CA3159CD51FE191D6E4538A18B37CCC309F59C29C6C45B7A17E1D78861E308A31DEB1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/built/csp/schedule.css?v=c1a593
Preview:	@import url(https://fonts.googleapis.com/css?family=Source+Sans+Pro);./*!. * Bootstrap v3.2.0 (http://getbootstrap.com). * Copyright 2011-2014 Twitter, Inc.. * Licensed u nder MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */./*!. * Generated using the Bootstrap Customizer (http://getbootstrap.com/customize/?id=7130 2de5c334d16fa768). * Config saved to config.json and https://gist.github.com/71302de5c334d16fa768. */./*! normalize.css v3.0.1 | MIT License | git.io/normalize */html{fon t-family:sans-serif;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,nav,section,su mmary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{ background:rgba(0,0,0,0)}a:active,a:hover{outline:0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:700}dfn{font-style:italic}h1{font-size:2em;margin:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\screen-collect[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 452 x 310, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	14355
Entropy (8bit):	7.961692305688219
Encrypted:	false
SSDEEP:	384:ZPiY6GoAwh/Q6NworbdhI3P9yIPEerMhKVo:ZCh/JwqRC/9/nrK
MD5:	915B0D966FEB045DFED4E8ACAFE1A5BA
SHA1:	F351F01DC034FD89BC208AD95AF7C1E8EC8813A3
SHA-256:	F94953ACF2BCD109074F5436E5F2FA2CF30703674565E90460D4524040DA9C57
SHA-512:	06FE80EFAF6990442554E6E4586F6C682B2BE2D1A99B46692F4D290A743889870E52C01B843AFCA8D283BD2BB5122622EB610A046C3B75090C889608D9349386
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/screen-collect.png
Preview:	.PNG.....IHDR.....6.....?....gAMA.....a.... cHRM..z&.....u0...`..:....p..Q<...OPLTE.....UUU@@@.....333.....***$$$... ....lll...~~~.....uuu.....vvv..... .....pp.....10.....qp." ....A@.....po....."".....y.....tRNS.....} {.....bKGD...-.....pHYs.....tIME.....4....".4.IDATx..}.c.....>A.....;.)..._r...D..i3.,.a6..d..l..$%..B.....W.>.....Y,Hb.....f$bw.3..of..o..)...k..T.(..S *.@T *....)..S *....D....). ...D..r.D....D....].....W.6|E.0....LH.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\screen-organize[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 426 x 310, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	8447
Entropy (8bit):	7.937549655107248

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\screen-organize[1].png	
Encrypted:	false
SSDEEP:	192:WNUSt0WARs+VUhopsuoITOrWeACPC2W8gQlG:WNTt4W+mhLmOtAMlG
MD5:	BAD5DA5083E2BD5C4B476B313D847E91
SHA1:	BCE32BD2B757CE89D1BD08D6EB8CBA13C18048A2
SHA-256:	51F1F00335EB255DF5412A10329A4BF7F351DB111C7416E57A34026909323172
SHA-512:	9783EC1A034AF6C9214C6929544F8FC0A1CC47C593204764FB0CDAA71CB4F731B79BAEFC28CE8799EB537B21FC4FC9D0A2FA166B765CAC7A79C1F95F06A83AB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/screen-organize.png
Preview:	.PNG.....IHDR.....6.....&.....gAMA.....a.... cHRM..z&.....u0...`..:....p..Q<..."PLTE..... ....{<.....bKGD.o.0O....pHYs.....tIME.....6*#.8 ....IDATx..]....q>...irm)..8n\Y...Z.T;....8.I.\.....6..%...@.....D..HE.T....4HIT....._g....1.....YMcbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbz.h...O..~..C....D....a..v..'.0 .E....{B..)..}...nm. ..}K.....d.+.(..bg`x.....g.3B...w.....j...o.|..3..w.64<.E..[.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\6xK3dSBYKcSV-LCoeQqfX1RYOo3qOK7j[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20180, version 1.1
Category:	downloaded
Size (bytes):	20180
Entropy (8bit):	7.97320012816743
Encrypted:	false
SSDEEP:	384:S3ECNC9EU5uXBx/d17jzOBmhUXQOTF3IHrYZEFeWXU5ebGLtCjUdtjVOTg:S3EC2rMXBdjzOBRx3IHrYOFeWLotCYL7
MD5:	5CC3AAE674EA3B199313B3B83BD795BC
SHA1:	993DB0EC4347B0CC53128CFDCBB767606D8A3576
SHA-256:	38399EFE707A8FFC12359A0086E7340315B42194A10FD2E1D1288BE12DA9E39C
SHA-512:	2346622E53705ABB58BDC45818D497CB17E9F9869B546CAF298D1E4D4A2D7E15B5A3C3EE8E6779D64C4C4BB0F98A58216A394BCA81F6660AE137FC6326B4895
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/sourcesanspro/v14/6xK3dSBYKcSV-LCoeQqfX1RYOo3qOK7j.woff
Preview:	wOFF.....N.....GDEF.....6...F....GPOS.....f.x.{GSUB.....{... J.c.OS/2...8...V...`[.t.cmap.....3cvt .....*...*.''..fpgm.....s.Y.7gasp.....glyf... ...4...f.....head..E....6...6....hhea..F.... ...$....hmtx..F .....P.=).loca..H4...''...*.s.Tmaxp..JX... ... .3.zname..Jx...A....[.s.post..K.....SF.prep..N....S...V.c..x....@....{..::#0. ZGK..`....R...^qT..qW<^...../....x....a.....f.]C..fe.5fs...m.a<]Cv}...7..NG..7l.#.}&..J.....^c.S.....>..yv.<{.C...N...p@...>....$..!.....:...BH...p.C.}).O/..M...t...TB....E...t.....s..L.H _..G3.I.....l?..y.`.....=.....Q.6.e....v.n.]T.....}w..iz..czc;.....C....Z6...m.2G|....b.8....x|I'T..Lb%.xI'Q.H.p.%...''UbH.$.%..I&SR.&.4.$...RP2($a..4JJ.e$...M9...DSA..(.T.< *S.xjI:Mh..vD.^.. !t..)t.'i./..`....&.1.%..L".)L.a.8.....#...@|...''.Y....J..$.....f%k.a.d.N<...r..6.#...}.gf~S.9.....A.A..affff~.....Y.TZ..j....E..N...pO.I..Ze).....`.V..[.c.W.10./.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Clarkson-Light[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 55115, version 1.1
Category:	downloaded
Size (bytes):	55115
Entropy (8bit):	7.988433188351148
Encrypted:	false
SSDEEP:	1536:SkaACTO1ukqstofyqxGOoisybru356+Vm8hghY4:SkaACmNuN+qp+pgH
MD5:	2AD9857AD748BE35101DEBAB00E5A092
SHA1:	B85D0B9E83CA83327D545938345ED0A5CB9CE449
SHA-256:	1A97919730ABCC084F8B59C1F3C9F99E22118BC1D85FECC5A67D9F9890F4EE39
SHA-512:	97222AF9C3B384C4E7B8788BFC29371DA45D18E718B005FD5490C1EA6EAC3E0C62B136CCBA634CFCBC2FF0BEA368A7877BAFABC1A283FDD6B3D1C08E3D3E5EA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/font/Clarkson-Light.woff
Preview:	wOFF.....K.....D.....;.....DSIG...<.....GPOS.....&.....J.X.GSUB.....,...LTSH.....?..{dOS/2...$...\...`..a,cmap..1.....''.cvt ..6....F...F...Afpgm..4.....s...7 gasp...t.....h.&glyf..;...b ...p{..Ahdmx.....*%..^...!xhead.....6...6...Ihhea.....!...$....hmtx.....p....g.=.loca..7....w...x....maxp..... ... .U..name.....v..Rpost.....N.p prep..5.....o<.....B...._.<.....C.....Z..B.....r.....x.c`d``>.....?..},...''.....G.....;.\...^.....]....x.c`a.g.a`e`a.b.```...q.F.6..L.,,. .....B5P...3....2600.....S.....ArL|L.. .7.f...x..Vmh.e.....YYS.67.v.g.9g..L.3..AQ.y...*Gk.....$.....#A..c.G...VD...$.%f*d.4...2..9.9...u..z..>_.}....B..g.r.....Vh'.^7.z..8.^.....}.. $....M.c..#-.Q.mh.4.....$t.:.*....s...]..z..c...r.. .f4.X..0...U/...M..V....$D.BT_.....|.\...:.n].>.r...|..Nr..B.....''.N;?.Zr..o.&..sHs.....'....II .q.f.....+....1..M...q...N..3.x.xD.a.....C.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Clarkson-Medium[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 56416, version 1.1
Category:	downloaded
Size (bytes):	56416
Entropy (8bit):	7.989848369901135
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Clarkson-Medium[1].woff	
SSDEEP:	1536:D5daVflgpie08IusbI7yt2xaGThBbg9Ru356WGJjn0X:D5didgpVL9etiam4jZ4X
MD5:	4F60EDF2654A7B4F8F5B383E1B2E6D63
SHA1:	DA17D8E0246A3A9C72861B6696CE28983BAB8E21
SHA-256:	B1EE6A1C6DADE765F8005823CAA0A961F22F0876C298DF168A49C6E05F11C049
SHA-512:	850985B4EC49D8F4CC0D35A4296899D6097EC282555FDE5A7FE506CBD91463E9A32FEF0065D3DABB70A4C89829E4BD19B8C66ED8F6CE1ABBD851AD8A27696F FB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/font/Clarkson-Medium.woff
Preview:	wOFF.....`.....\.....X.....<.....DSIG...P.....GPOS.....)....V.Z..GSUB.....,...LTSH.....?...OS/2...$...\...`..c5cmap..1 .....".cvt ..6....D...D....fpgm..4.....s...7g asp.....h.&glyf..:...d....d.s..hdmx.....)s..\H.|."head.....6...6... hhea.....!...$....hmtx.....h....{h+4loca..6`...x...x..D.maxp..... ... .U.uname.....v..Rpost.....N.pp rep..5.....U.....B3c.t_.<.....Z.....m.....x.c`d``>.....?...,..".....;.]...]....x.c`aR`.....m.....X.A.e.....j... f....el``.....g.....&.....)..n.. ...x...mh.U....'.....w.nw.....u..-.nd.*...K*.V"H.O.@.P..^...H...|Q..Io"B"."....\,o.s...y..|..s.....=.kV(....D4`^S.M.6.Q"8..=..]P....3gT..N]...6.we....f.k..R..a....nd|...*;.;h.+..9..c3..c.L. .....d..;A...J..5h...)j_..1.><.'.~.N....f.....K.sT...c..0.m..^..5v.j...;.Q..7.);.F.....Q.X.....v6x..#`.....`..y....o...n..6.RsII..)...Z..u

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\TV4F7E56.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	49741
Entropy (8bit):	5.396289523498696
Encrypted:	false
SSDEEP:	1536:nytMPNAK29qWqNkMyb1K0+/RVaKNZKP20MHrJYnXmuEHGQ15:/LkWHLv
MD5:	B34C43F12AB62EB45DF01B1D4E898F5A
SHA1:	9B3606A6E4739CA66F9EAC8A8D96082FF0FEACE3
SHA-256:	5380BBBAAEE98F340568B913BC1058399890086248F1936A7AEBF6F7FD1C4668
SHA-512:	985D75C425DA08CD99BBF64D55E9322E1AABEBCF8C3C89368CD491E3B2CDF1CBCB21421A9666406F7DAC53C14D8A7930B6B407C4E91F1AE4A8E7ACDBD7D3 3BA
Malicious:	false
Reputation:	low
Preview:	.<!DOCTYPE html>.<html lang="en">.<head>..<script...src="//consent.trustarc.com/notice?domain=squarespace.com&c=teconsent&js=nj&noticeType=bb&text=tru e&pn=2&gtm=1&pcookie"...crossorigin="">..>..</script>.. Google Tag Manager -->.<script nonce="337fe7bf64041c273f10c35acf7ff998a825d05d36620acec023810 3772c25bad54b6366350364d01a63107e45c1a3adef6e92cd66216b62faf0675419ce3d50">..(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':.new Date().getTime(),eve nt:'gtm.js'});var f=d.getElementsByTagName(s)[0],.j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src=.'https://www.googletagmanager.com/gtm.js?id='+i+dl ;f.parentNode.insertBefore(j,f);.})(window,document,'script','dataLayer','GTM-5G77WWT');.</script>. End Google Tag Manager -->..... Start Visual Website Optimizer Asynchronous Code -->...<script nonce="337fe7bf64041c273f10c35acf7ff998a825d05d36620acec0238103772c25bad54b6366350364d01a63107e45c1a3adef6e92cd 66216b62faf0675419ce3d50">.....var _vwo_code = (funct

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\client-login[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	10724
Entropy (8bit):	5.335893597777599
Encrypted:	false
SSDEEP:	192:Nd+z7/QfoGe4poCjiDoJQdpo8gXH0ffJpHxR+Mp8k47DT0XtlhpC9mHBWw9qGzoz:L+z7+oGdpDhQdpTcH0fPNpGT09npnha5
MD5:	4491B89D8941EDCFC4E2589D9D5DE311
SHA1:	1A9B3EBACB9FE980E90BEA8059CD6ACAAB2B3DDB
SHA-256:	B109F557EE1439FDEE043DB13BC3CEB6DB085AD55CF97C0F8276F5AD7F9BB156
SHA-512:	901744636270CBB444213A7B5735527EAC9D870EE2B3B7FBD4D39C5826EC8F02ECB3F268C466F9795DC93924275EF24FDBA9C8DFC2050CDDAFD18F9C2AF83D B
Malicious:	false
Reputation:	low
Preview:	...<!DOCTYPE html>.<html lang="en">..<head>...<link rel="canonical" href="">...<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />...<title>Schedule Appointment with Health Department of Northwest Michigan</title>...<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=2.0">...<meta name="referrer" content="same-origin">...<meta name="format-detection" content="date=no">...<meta name="description" content="Schedule your appointment online with Health Department of Northwest Michigan" />...<meta property="fb:app_id" content="465400520261032" />.....<meta property="og:type" content="website" />.....<me ta property="og:title" content="Health Department of Northwest Michigan" />...<meta name="fb:extensions:title" content="Health Department of Northwest Michigan" />... <meta property="og:description" content="Schedule your appointment online with Health Department of Northwest Michigan" />.....<meta name="twitter:card" content="su mmary">.....<meta na

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\efreechurchdose1covid20210310[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	19904
Entropy (8bit):	5.290355043978193
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\efreechurchdose1covid20210310[1].htm	
SSDEEP:	384:F+zUfaphQ2OH0fSgRA4EfSmmS9E4LrozZfjbp7Es8eoA09nfhaso6GPpM:F6Ufa5OU6Tvo4Lc81ASnZas9GP6
MD5:	588ACDAD0F456D7322C12365DB5F0305
SHA1:	D60F5B7AF64314D541BFCFD64694FE9AA63AA962
SHA-256:	28E159C59B25797A3EAADE51A21453F078E9BBBF179DC7BBB39DCC7FAD450B39
SHA-512:	3A75D192A27A0E46C1CF713E5956BAEC3553091545C8A88144821BC778EE9122A0528A5A10D4FE5E208F9046E8177404EB3D8D70931DEB0CCE6CE4DE0A63119
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html lang="en">..<head>...<link rel="canonical" href="https://app.acuityscheduling.com/schedule.php?owner=21613168">...<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />...<title>Schedule Appointment with Health Department of Northwest Michigan</title>...<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=2.0">...<meta name="referrer" content="same-origin">...<meta name="format-detection" content="date=no">...<meta name="description" content="Schedule your appointment online Health Department of Northwest Michigan" />...<meta property="fb:app_id" content="465400520261032" />.....<meta property="og:type" content="website" />...<meta property="og:url" content="https://app.acuityscheduling.com/schedule.php?owner=21613168&q=efreechurchdose1covid20210310&calendarID=4953566" />..<meta property="og:title" content="Health Department of Northwest Michigan" />...<meta name="fb:extensions:title" content="Health Department of Northwes

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1130
Entropy (8bit):	7.774023477258517
Encrypted:	false
SSDEEP:	24:V99gwbQM8r53dYnE+Yif6UFTKzSURuVRkOFoqN0ryNu:L9TbQhr5dME2f3FTgRKqVKc
MD5:	9E692FE534DA39B5C8F14625EB830C64
SHA1:	98CFEE2A58D900D55519E731D87AD678B5BE04FC
SHA-256:	6F18DCF9C7761928B5A69D498370F1C566EEF18BCAC4BFF21D7336AC63618D17
SHA-512:	372AA1710AFAE9A595DFE7AD131F0CA1DCC1C4A15206ECCD448CC580943D5D3367B882A1EF7A123DBECEF2CE5AA39040B2CC587125F8C12F4002E8C50B2F803
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.acuityscheduling.com/favicon.ico
Preview:	.PNG.....IHDR...0...0.....W.....sRGB.....$IDATh..Xi..Q..... KvF.(..(...EI~..P...BY..0Yj0.....2.?$Y..SLh,%d.c{.}...:...w..[.=.].....w...T.....f .3."...F.!.[.....@.Q)2.....?.....%@..28...\l....9...rB.1.'..`Xy.b,..O...U%..~....:.D=.L..H....z...c.0.t..".s..~F..N.Y..@w....&.%.c.7.....P.....F....>.D.....v`Y.....I..{..[P.4}.c.miV.....oU.*9C.s..y...W..A...Y.4...Kp..({>hhV.f.8.....oZ..Y.b.M.f.. :.....ANA.^0.A...8r[..>.?..*...)P.q.u;....'[..6..Y.u".....mK9...5...b.Bx.@....m.....v....6;.....x...B...@.]..P.r(m.....\.;..B..|...WI..v.\.W:.x..]..P.7.m.y!.M..i..i..Ya.....Z.Xl\...+.....+.K.>:...L.../....2{..x.....6.g.....q...N.cwm.....ty..%-eg=....o..&X&. 8...W....#.....t2i.....T[.x7..$Bg...,?6.....L@.m.).....z~#'F.....7@./*g.Uq.@..c..0..i..$Q...%..btl..].....M.B;'...w.....*..>..t9.....V.F..#....|=.....S.....ja3....*. ...L..).M..@..L...+.....>....W..q.|...J}.xY..&K.p5...:P....y@..eB.>.z.0. ....?.?Q.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\get[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Clarkson T
Category:	downloaded
Size (bytes):	133016
Entropy (8bit):	5.390975903073818
Encrypted:	false
SSDEEP:	3072:RgDV2ab+vhI62GrpCGsMSBe4IiK1eBmgEtx:CDr+p2SsrFqePEP
MD5:	B15318518B0FC02E41E21D7BB2F21C45
SHA1:	72C3E0D5542824492787FE70B69E8948CAB9C5FA
SHA-256:	5BDAB82724BD5453B2B828AEE84C064839468E7B7D50417BB406946FE1BD01E1
SHA-512:	7B3E63046FFA7E6D0F3B62297F10CE91EF9C716CDE2DBBB6AE314845A2957A51E5C87DA49A501B32F1D40967D3DF8A732D7BF9172E5EB2DC2325F08F10292F4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://consent.trustarc.com/get?name=ClarksonTT-Light.ttf
Preview:	.....0DSIG.....GPOSJ.X...dH....GSUB.....d...,LTSH..{d.....?OS/2..a,.....`cmap"...k.....cvt ...A..sT...Ffpgm...7..o....sgasp.h.&..d8....glyf{..A..x....phdmx..!x...D..^.head...6...<...6hhea.....t...$hmtxg.=.....loca.....s....xmaxp.U..... name?\MP..J....)post.N.p..S.....prep.o<...q`.....B.`?._.<.....C.....S..B.....r.....B.....;.\...^.....]....,.....X...K...X...^.2.<.....@. {.....OPTM..... ..... .....].`.A.6...;.".?."../...A.".".".'.6.2.....E...D.....d.<.....5.1.<.+.$.":.,.X.;.....O.7.X.5...E...&.6.@.6.2.6.j.....>.....a...3...a.a.a.9.a...3...a...a...$.s.a.*.a...a...a.(.3.\.a.).3...a.a.(.G.....Y.....$.r...n...N.#.7.].....7...6./.0.%.e.<.6.-...Q.<.-...-.W.-,.#../.R.R...R.....R...R...Q.T.Q.k.-...Q...-.k.Q...#.=...M.K.....$.,.#...].,.'.6.(.....V.6...6.+.6.%.6.....].6.A...h.V.0...2...$.6.....E.V.0.f.1...-.6.>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\logo-ga[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	6661
Entropy (8bit):	4.102338735832785
Encrypted:	false
SSDEEP:	96:3nqkB8cll5lby4iz6gSBbAsO+W5ZeEUDw2qxrU7+Fq4REL1DXZq4RoF:3qkB8cllDVgzSB7rqz3U7MWs4+F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\logo-ga[1].svg	
MD5:	57EB73BEC651BD0D72A974BCED5726E6
SHA1:	790E9C858C4EABE99D3C5D6E94BFD7DF651288D7
SHA-256:	C4F73421F96F871CD958FE9935B032407AC0E08816936CE388ED2D8330A39F36
SHA-512:	E01451C14BF13FEFE69A5C598C2431BE806E98E72A472855C7407F736A5E40C2C16BB173A3348B42A7AF2721DED97581BB8CB4D5DDB51A8F049A4DC594F266E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/logo-ga.svg
Preview:	<svg width="91" height="67" viewBox="0 0 91 67" fill="none" xmlns="http://www.w3.org/2000/svg">.<path d="M46.999 56.3572L48.5464 60.451H45.5483L46.9987 56.3572H46.999ZM46.4189 54.9957L43.0341 63.9637H44.2914L45.1616 61.5273H48.9296L49.7998 63.9637H51.057L47.6723 54.9957H46.415H46.4189ZM64.696 63.9637H65.8566V54.9957H64.696V63.9637ZM52.8013 58.6969C53.1881 58.1121 53.9619 57.6245 54.7351 57.6245C56.2824 57.6245 57.0563 58.6968 57.0563 60 .2561V64.054H55.8957V60.4514C55.8957 59.1841 55.2189 58.6969 54.3483 58.6969C53.3815 58.6969 52.7043 59.6714 52.7043 60.5492V63.9608H51.5437 V57.7266H52.7043L52.801 58.7011L52.8013 58.6969ZM58.0267 62.1078C58.0267 60.7463 59.284 59.9634 60.7343 59.9634C61.6045 59.9634 62.1846 60.1583 62.3784 60.3532V60.1583C62.3784 59.1838 61.6049 58.6965 60.831 58.6965C60.1542 58.6965 59.5737 58.9889 59.3807 59.5736L58.3168 59.0863C58.5102 58.5016 59.2837 57.6245 60.831 57.6245C62.2813 57.6245 63.5386 58.5016 63.5386 60.2561V63.9601H62.4747V63.083H62.378C62.088 63.5703 6

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\logo-paypal[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	9575
Entropy (8bit):	4.182750127328269
Encrypted:	false
SSDEEP:	192:MlN+OslrlGin1FXDJ99XLJD8ncKO++ITrlNazLCYcZdant+JeMnc:MlNPGWX399DtKO/YlNazLCYcZEtsnc
MD5:	D11A46BAF4FCB71B85E3C8C916B142B3
SHA1:	DC5E1AC0E437CDA5F497DABE78B5F866B55216D7
SHA-256:	3AE3EEB30CD6B730BA42528CC9761C1A2064C04576A2A47703FFEEF528428F0D
SHA-512:	127090EED85E1272E7062457F904B03A7405DD436928633F5DB2178B941E022F6DA7A15CD7D0F61D2E35A694C9525D87993DD0984F2CA15F99BCD4ACEC9F50D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/logo-paypal.svg
Preview:	<svg width="113" height="30" viewBox="0 0 113 30" fill="none" xmlns="http://www.w3.org/2000/svg">.<g clip-path="url(#clip0)">.<path fill-rule="evenodd" clip-rul e="evenodd" d="M21.1576 3.16514C19.8488 1.64951 17.483 0.99939 14.4558 0.99939H5.6724C5.0542 0.99939 4.52684 1.45682 4.4306 2.07796L0.772955 25.6435C0 .756054 25.7531 0.762671 25.865 0.792351 25.9717C0.822031 26.0783 0.87407 26.1772 0.944887 26.2615C1.0157 26.3457 1.10362 26.4134 1.20259 26.4598C1.30 155 26.5062 1.40922 26.5302 1.51819 26.5302H6.94115L8.30228 17.7528L8.2607 18.0285C8.30661 17.7282 8.45652 17.4544 8.68338 17.2567C8.91025 17.0589 9.1 9913 16.9501 9.49788 16.95H12.0746C17.1373 16.95 21.1014 14.861 22.2585 8.81803C22.2939 8.63944 22.3231 8.46556 22.3493 8.29559C22.203 8.21726 22.203 8.21726 22.3493 8.29559C22.6942 6.06169 22.3462 4.54135 21.1576 3.16514Z" fill="white"/>.<path fill-rule="evenodd" clip-rule="evenodd" d="M87.5441 14.3785C87.21 23 16.5904 85.5501 16.5904 83.9426 16.5904H83.028L83.6693 12.4618C83.6882 12.341

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\logo-stripe[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	2533
Entropy (8bit):	4.533191748914814
Encrypted:	false
SSDEEP:	48:w2Rwkt2vLjA896Y6OXxqpbIgutaazB899N9dHaq9O:fZt2vLEsdA+zW/d6r
MD5:	5D5311835AD431BEA17AC2BF394C2DA1
SHA1:	F6D561B7BC3FB03D97D628988B644082DD63F6D9
SHA-256:	FA70690521BEA1925D90962AA6B9CF29347FCD355012336663C945FE4CBEE073
SHA-512:	2F457338FD941BD542B6CDD8366D31DB7DE551F0399BEAEA3976273482747FE252195707CF16708EE713ED56F84681070A8E818BA8E36C8CEA2CF998D3DF1061
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/logo-stripe.svg
Preview:	<svg width="80" height="34" viewBox="0 0 80 34" fill="none" xmlns="http://www.w3.org/2000/svg">.<path fill-rule="evenodd" clip-rule="evenodd" d="M79.4602 17.662 5C79.4602 12.0818 76.757 7.67828 71.5905 7.67828C66.4023 7.67828 63.2631 12.0818 63.2631 17.6189C63.2631 24.1805 66.969 27.4941 72.2881 27.4941C74.8823 27.4941 76.8442 26.9055 78.3266 26.0771V21.7172C76.8442 22.4584 75.1439 22.9162 72.9857 22.9162C70.8712 22.9162 68.9964 22.175 68.7566 19.6026H79.41 66C79.4166 19.3192 79.4602 18.1857 79.4602 17.6625ZM68.6912 15.5915C68.6912 13.1282 70.1954 12.1036 71.5687 12.1036C72.8985 12.1036 74.3155 13.1282 74 .3155 15.5915H68.6912Z" fill="white"/>.<path fill-rule="evenodd" clip-rule="evenodd" d="M54.8483 7.67828C52.712 7.67828 51.3386 8.68107 50.5756 9.37866L50.2922 8.02708H45.4963V33.4456L50.9462 32.2902L50.968 26.1209C51.7528 26.6876 52.9082 27.4942 54.8265 27.4942C58.7287 27.4942 62.282 24.3551 62.282 17.4446C62.2602 11.1226 58.6633 7.67828 54.8483 7.67828ZM53.5404 22.6983C52.2542 22.6983

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\marketingsquarespace.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	74698
Entropy (8bit):	5.125177830908476

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\marketingsquarespace.min[1].css	
Encrypted:	false
SSDEEP:	768:MUrfsLRw+F+M+HiOX434SkkOIg8amyXosnQUvU59P7+E447YUpPXw7l8w/jsdwx2:MUrULRGkzHlz
MD5:	B1A2D403C6920B07BC6EBE008A0FF33B
SHA1:	F94DA16A85F58925B72E86B44B6EEE2E8A50D0C1
SHA-256:	B53E92927A137BF24B4DC9C9404EA925F3754C5C940055DB67C58C0508FE30BA
SHA-512:	93396A87A87D993EA2FC4CA71570C0C29351528B196018C46BF001D414215FD484D7EC577B8B5C4F9D0208885457A6CA89864FDECDF4E4728D6670AB18D712E(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/css/marketingsquarespace.min.css?v=c1a593
Preview:	@import url(https://fonts.googleapis.com/css?family=Source+Sans+Pro);*{margin:0;padding:0}*,:after,:before{-webkit-box-sizing:border-box;box-sizing:border-box}html{-webkit-text-size-adjust:100%;-ms-text-size-adjust:100%;-webkit-font-smoothing:antialiased;-webkit-tap-highlight-color:transparent;overflow-x:hidden}body{font-size:1rem;font-family:Clarkson,"Avenir Next",-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,Oxygen,Ubuntu,Cantarell,"Fira Sans","Droid Sans","Helvetica Neue",sans-serif;line-height:1;background-color:#fff;color:#222;overflow-x:hidden}input,textarea{font-family:Clarkson,"Avenir Next",-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,Oxygen,Ubuntu,Cantarell,"Fira Sans","Droid Sans","Helvetica Neue",sans-serif}.cf:after,.cf:before{content:"";display:table}.cf:after{clear:both}.cf{zoom:1}.container-fluid{width:100%;max-width:1680px;padding:0 40px;margin:0 auto}.container{width:100%;max-width:1170px;margin:0 auto}.btn{display:inline-block;padding:15px 20px;margin:0 0 2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\schedule[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	19872
Entropy (8bit):	5.2934893754734595
Encrypted:	false
SSDEEP:	384:F+z8haThQ26H0fSgRA4EfSmmS9E4Lro1Zfjbp7Es8ko2q9nBhaso6GPpM:F68haX6U6Tvo4Ly8n2gn3as9GP6
MD5:	90D4B55E9BF53A30757EEA343B3E796B
SHA1:	E97B86530F2301E626C3C8DACF72E89C177065F4
SHA-256:	D58082F9020B3BBCE529F5AF3AE5EA05032E1D1877BF4D00FCD6890045279114
SHA-512:	8D40A8D739903ACA9D4C1CD544AAE1C2886BC156441EED657804C879166E5B835A4F4E6B22CC61081E308F2D2B8B1399B97BA2A9E25120163E42C49B6392417
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html lang="en">..<head>...<link rel="canonical" href="https://app.acuityscheduling.com/schedule.php?owner=21613168">...<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />...<title>Schedule Appointment with Health Department of Northwest Michigan</title>...<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=2.0">...<meta name="referrer" content="same-origin">...<meta name="format-detection" content="date=no">...<meta name="description" content="Schedule your appointment online Health Department of Northwest Michigan" />...<meta property="fb:app_id" content="465400520261032" />.....<meta property="og:type" content="website" />...<meta property="og:url" content="https://app.acuityscheduling.com/schedule.php?owner=21613168&calendarID=4953566" />..<meta property="og:title" content="Health Department of Northwest Michigan" />...<meta name="fb:extensions:title" content="Health Department of Northwest Michigan" />...<meta property=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\swipe[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	8075
Entropy (8bit):	5.2675626646734
Encrypted:	false
SSDEEP:	96:wqGrP97K/lpHeaDcFShwFMK8ODZzPjH1csVyr0YVTPK6OneZ/Uv:wFrlm/ixS6M1A5b1pVy5VTPZOnfv
MD5:	C7AAFC5AF66A76EC62F531CEEBBAAC89
SHA1:	1717311661A7AA5774BF5EE910007AF0838CF256
SHA-256:	AB359967B981ADFFB7453EF1BE751A52DE78A1BDA87EC22E6019F13090F5DCD2
SHA-512:	8CDCE44A14D9FBD5DAEE14547466D1BAD9DCF1312492FC273AF72E2EDBC642801BAAB2DB791336A29AAAE5296444E328060729A9331AF86A9F6B8A5F5E25A4B0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/js/swipe.js
Preview:	!function(t,e){t=t||{},"function"==typeof define&&define.amd?define([],function(){return t.Swipe=e(),t.Swipe}):"object"==typeof module&&module.exports?module.exports=e():t.Swipe=e()}(this,function(){var t,e="object"==typeof self&&self.self===self&&self||"object"==typeof global&&global.global===global&&global||this,n=e.document;function i(t,i){"use strict";var o,r,s={},a={},u=(i=i||{}).auto||0,c=!1,l=function(){},v=function(t){setTimeout(t||l,0)},d=function(t){return!!t&&("boolean"!=typeof t.cancelable||t.cancelable)};Element.prototype.matches||(Element.prototype.matches=Element.prototype.matchesSelector||Element.prototype.mozMatchesSelector||Element.prototype.msMatchesSelector||Element.prototype.oMatchesSelector||Element.prototype.webkitMatchesSelector||function(t){for(var e=(this.document||this.ownerDocument).querySelectorAll(t),n=e.length;--n>=0&&e.item(n)!==this;);return n>-1});var f={addEventListener:!!e.addEventListener,passiveEvents:function(){var t=!1;try{var n=Object.defineProp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\tippy[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	53091

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\tippy[1].js	
Entropy (8bit):	5.2509747873352515
Encrypted:	false
SSDEEP:	768:NLsgyziJ/0D45sxpOxvYD73Y5v9zwL9TilDzf9tnjw4OyMAjg2CdbiLUrNTji+QZ:NLnyzi90D4DWLQza/9IENmvfa0
MD5:	88D62DCC2558466476BE7AB9797D4704
SHA1:	38691B4F8C2D276CB18B4A236F6D6850B66143AF
SHA-256:	90767F34110F4676BBFB317C848696678ABF4D8F4BFF4E2DA81BD1E3E6BC8EE8
SHA-512:	4D44B64CF3B84269BA076C8D342C301B11D8D1EA45203426C56BB305A7584DC498829B1078E15CA8829DB56DACBE314AD2A02D721F70AAE035FA4BC612B5A1 4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/js/tippy.js
Preview:	/*. Copyright (C) Federico Zivolo 2019. https://popper.js.org. Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT).*/. (function(e,t){'object'==typeof exports&&'undefined'!=typeof module?module.exports=t():'function'==typeof define&&define.amd?define(t):e.Popper=t()})(this,function(){'use strict';fu nction e(e){return e&&'[object Function]'==={}.toString.call(e)}function t(e,t){if(1!==e.nodeType)return[];var o=e.ownerDocument.defaultView,n=o.getComputedStyle(e,null); return t?n[t]:n}function o(e){return'HTML'===e.nodeName?e:e.parentNode||e.host}function n(e){if(!e)return document.body;switch(e.nodeName){case'HTML':case'BODY' :return e.ownerDocument.body;case'#document':return e.body;}var i=t(e),r=i.overflow,p=i.overflowX,s=i.overflowY;return /(auto|scroll|overlay)/.test(r+s+p)?e:n(o(e))}funct ion r(e){return 11===e?pe:10===e?se:pe||se}function p(e){if(!e)return document.documentElement;for(var o=r(10)?document.body:null,n=e.offsetParent||null;n===o&&

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\amplitude-7.1.0-min.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	61487
Entropy (8bit):	5.486482424874459
Encrypted:	false
SSDEEP:	1536:z+9M1K3WS4ylpQ0YgRBQ/DeXACzSXnDchzQ3pyMtgRu:zvupQ0ADexC
MD5:	16CCFCE335CFD5A79A18193A77B65526
SHA1:	2FFF64B480ED24CD411E398DA1DC45A891847ACF
SHA-256:	A9A2E998EE0FD7C858904E6A1ECE449C07DEA8477A51AA735B7EF1187742A102
SHA-512:	F710CC14F83C86648F07743B67D09905676027BA00603A90A95379A9EA14AF7739B3C75E10A426AFEDD7FEC2370425D2769D88CD86C814D48BB28C58A8DE2309
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.amplitude.com/libs/amplitude-7.1.0-min.gz.js
Preview:	var amplitude=function(){"use strict";function t(e){return(t="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(e){return typeof e}:function(e){return e &&"function"==typeof Symbol&&e.constructor===Symbol&&e!==Symbol.prototype?"symbol":typeof e})(e)}function i(e,t){for(var n=0;n<t.length;n++){var i=t[n];i.enumer able=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(e,i.key,i)}}function o(e,t,n){return t in e?Object.defineProperty(e,t,{value:n, enumerable:!0,configurable:!0,writable:!0}):e[t]=n,e}function v(t){for(var e=1;e<arguments.length;e++){var n=null!=arguments[e]?arguments[e]:{},i=Object.keys(n);"function "==typeof Object.getOwnPropertySymbols&&(i=i.concat(Object.getOwnPropertySymbols(n).filter(function(e){return Object.getOwnPropertyDescriptor(n,e).enumerable}))),i.forEach(function(e){o(t,e,n[e])})}return t}var g={DEFAULT_INSTANCE:"$default_instance",API_VERSION:2,MAX_STRING_LENGTH:4096,MAX_PROPERTY _KEYS:1e3,IDENTIFY_EVENT:"$ide

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\ask[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 660 x 642, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	15744
Entropy (8bit):	7.9261740366133155
Encrypted:	false
SSDEEP:	384:snbZhQWqsHgQEoXNqb5F9YzBRPHbZ6vQJ8/+tGq1u5G88vFTb:EXqzwXNqb50FRPHbZ6vQJicUqvFTb
MD5:	C55A0C260863911C82B5A76A2CFF1931
SHA1:	972B4C000AC226AAD05C9C754DE8BCBCF2E92D03
SHA-256:	ADAAC99936EB9C888CB9CC6C2912252449C031D9B13F0D0BB2C9904FABD1CBC6
SHA-512:	0522E8537148A8EF68F1A75880B1C8C18174B047047956E826E5F09F7F86E646B589C0343660710F2EA6BF823F9E818E98EBDC61C9A8BAD93AFA58641B7FEA5B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/ask.png
Preview:	.PNG.....IHDR.....X.....gAMA.....a.....sRGB.....KPLTE.....yyy.....QQQ.....ccc;;;...hn....pHYs..... .IDATx..r.0..].*...z ..._z3.H....U6.]..... h.$..?.....).).....).)....).).....).).....).....).).....).)....).).....).)....).).....).)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\efreechurchdose1covid20210310[1].htm	
Entropy (8bit):	5.295941077149533
Encrypted:	false
SSDEEP:	384:F+zUEKahQ2MH0fSgRA4EfSmmS9E4Lro8Zfjbp7Es8ZobB9nwhaso6GPpM:F6UEKEMU6Tvo4LP8+b3nKas9GP6
MD5:	80C42C9AEF76C51640C811B78FE7828A
SHA1:	ACD448E7D0C60871EF964A67116679A65C3039BC
SHA-256:	FD6EF2E69DDC09F7E18FFAE65B7F915323A3960AD1EB4E8CE73B8EAD5C416665
SHA-512:	74AA7C488B8D36C4CC2872733CC6CDE7950B37C0C7E945AA750790BBE8FAA309AA8832DCCD6C07364C8B576F94F84006C74981F2ED079E10A41043CE22797DA
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html lang="en">..<head>...<link rel="canonical" href="https://app.acuityscheduling.com/schedule.php?owner=21613168">...<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />...<title>Schedule Appointment with Health Department of Northwest Michigan</title>...<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=2.0">...<meta name="referrer" content="same-origin">...<meta name="format-detection" content="date=no">...<meta name="description" content="Schedule your appointment online Health Department of Northwest Michigan" />...<meta property="fb:app_id" content="465400520261032" />.....<meta property="og:type" content="website" />...<meta property="og:url" content="https://app.acuityscheduling.com/schedule.php?owner=21613168&q=efreechurchdose1covid20210310&calendarID=4953566" />..<meta property="og:title" content="Health Department of Northwest Michigan" />...<meta name="fb:extensions:title" content="Health Department of Northwes

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\get[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Tfayzxghsxhzrjigoixtfuefbuz family
Category:	downloaded
Size (bytes):	84792
Entropy (8bit):	6.176366322347386
Encrypted:	false
SSDEEP:	1536:VtNSS+luxkDPRKk70zvuI62WvfPTbpF3WKpBlK4TDRp1c:gGDPRKWgvuI62GrbpF3pBo4/X1c
MD5:	294B786746B106445C16576BA95C410A
SHA1:	6B1C37F5554B37213F69F29B6751BC7D5883D5AE
SHA-256:	78325406E3168024D7AAA64DDFF5222841CBD90A06565AA7913E4AE94D7A7437
SHA-512:	FC08F962C102EE6ED99CA8467ADF2F60A603F592F4C6D466502FD14620155691324166B2E7DEBD38DA1BADACE3B0AC73054D50D87FA924178F9328A7A281486
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://consent.trustarc.com/get?name=Clarkson-Light.eot
Preview:	8K..(J.....,.....LP....{ .@..... ....B.j.....6.T.f.a.y.z.x.g.h.s.x.h.z.r.j.i.g.o.i.x.t.f.u.e.f.b.u.z.....R.e.g.u.l.a.r...2.V.e.r.s.i.o.n. .1...0.0.1.;. .b.u.i.l.d. .0.0.0.6.. .6.T.f.a.y.z.x.g.h.s.x.h.z.r.j.i.g.o.i.x.t.f.u.e.f.b.u.z.....DSIG.....J ....LTSH.).....OS/2..a-.....`cmap"...^.....cvt ...A..f....Ffpgm...7..b....sgasp.h.&..J.....glyf.l....jD...Hh dmx..@.....R.head...H.....6hhea...H...T...$hmtx..0.....loca:q.p..fT....maxp.....x... name.....4.....post.....=t....prep.o<...d.....Bj..B_.<.....C.....Z..B.....r..... .....B.....\...^.....]....."..,.....X...K...X...^.2.<.....@. {.....OPTM..... ....].`.A.6...;.".?."../...A.".0."."...'.6.2.....E...D.....d. <.....5.1.<.+.$.".:.,.X.;.....O.7.X.5...E...&.6.@.6.2.6.j.....>.....a...3...a.a.a.9.a...3...a...a...$.s.a.*.a...a...a.(.3.\.a.).3...a.a.(.G..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\logo-01[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3814
Entropy (8bit):	4.078694511993884
Encrypted:	false
SSDEEP:	96:goumIt0ir5NNjunRcRvafFFAVvDx7qTcmlV:WmBi5NJunRcRva9FIDx7qTcmlV
MD5:	DDBE8FF2E4785DF11FC236166A07DB2D
SHA1:	D2E50FFED9681423C332E06D98D3C78F92212789
SHA-256:	8ADFB8B060235F81967E73BBFEC4E257BA0AB13E488A4C9AE5210792500A077B
SHA-512:	31363833D287EC67A31CD86CF1CB5CB085C1C05462F823A08E70ADE83B7622899D272978DD0752C32BE5DE7EBCDC6209D2ED9EC10A4EF53C939FF598AAAF90B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ph-northwestmi.as.me/img/brand/logo-01.svg
Preview:	<svg width="200" height="22" xmlns="http://www.w3.org/2000/svg"><g fill="#313131" fill-rule="evenodd"><path d="M5.512 11.603l8.404-8.572a2.98 2.98 0 012.14-.903c.81 0 1.57.32 2.14.903l.654.668 1.31-1.336-.655-.668A4.797 4.797 0 0016.055.24a4.8 4.8 0 00-3.45 1.455l-8.403 8.572 1.31 1.336z"/><path d="M16.73 5.862l-1.31-1.336-8.404 8.572a2.989 2.989 0 01-4.28 0 3.134 3.134 0 010-4.365l7.252-7.397L8.678 0l-7.25 7.396c-1.904 1.94-1.904 5.098 0 7.039a4.797 4.797 0 003.45 1.454c1.303 0 2.53-.517 3.448-1.455l8.404-8.572zm8.365 1.534a4.796 4.796 0 00-3.45-1.455c-1.304 0-2.53.517-3.45 1.456L9.793 15.97l1.31 1.335 8.403-8.572a2.99 2.99 0 014.28 0 3.1 3.1 0 01.886 2.183 3.1 3.1 0 01-.886 2.184l-7.25 7.395 1.31 1.336 7.25-7.395c1.902-1.94 1.902-5.098 0-7.039v-.001z"/><path d="M21.01 10.228L12.606 18.8a2.987 2.987 0 01-4.28 0l-.655-.668-1.31 1.337.656.667a4.798 4.798 0 003.45 1.455 4.799 4.799 0 003.45-1.455l8.403-8.572-1.31-1.336zm14.953 1.402h3.5l-.577-1.717a137.39 137.39 0 01-.915-2.756h-.458c-.2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\logo[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\logo[1].svg	
Size (bytes):	11736
Entropy (8bit):	4.155371570154707
Encrypted:	false
SSDEEP:	192:7dH3XblyM74q2vrCWPYTanOild5wbcuS9DsTLEh4QJEOaEzt6/FM1naSHUxGB1Yk:8DeiJw4LDsUh4uIytUFE0oBkEsM
MD5:	8DCC6EE640B3A0873DB2CD12D24CE64C
SHA1:	137024194B22DE90F0DB33F9AE69D3D259BC10A4
SHA-256:	9F7EC21D7D5169533FBB0F74EA6F332AC0E8633E90B5C45AF54C8A45C5E52A70
SHA-512:	E8457B59F9E49CCA64A4B8FCB0648026C972E91E78C157B7DD63BD0BFB680F968F6BAD4DDA6A7F61CE075D17585775283DB51DF17B101A74CCE04A39AC6086A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.acuityscheduling.com/img/marketing/squarespace/logo.svg
Preview:	<svg width="230" height="33" viewBox="0 0 230 33" fill="none" xmlns="http://www.w3.org/2000/svg">.<path d="M0.175995 31.3941H1.46299L2.255 29.1391H5.676L6.46799 31.3941H7.832V31.0091L5.06 23.4961H2.981L0.175995 31.0091V31.3941ZM3.124 26.7081C3.498 25.6521 3.652 25.1901 3.828 24.6951H4.1689C4.32299 25.1681 4.51 25.7291 4.851 26.7081L5.27999 27.9621H2.673L3.124 26.7081Z" fill="white"/>.<path d="M12.4567 29.2711C12.7097 30.8111 13.8647 31.5701 15.4927 31.5701C17.2417 31.5701 18.4737 30.5911 18.4737 29.1171C18.4737 27.7421 17.6047 27.3021 16.1857 26.8621L15.6247 26.6861C14.7227 26.4001 14.1727 26.1911 14.1727 25.5311C14.1727 24.9481 14.6567 24.5301 15.4597 24.5301C16.3177 24.5301 16.7907 24.9151 16.9557 25.5751L18.2757 25.4651C18.1107 24.1781 17.1207 23.3421 15.5037 23.3421C13.7767 23.3421 12.6987 24.2881 12.6987 25.6081C12.6987 26.8621 13.5567 27.5001 14.9647 27.8961L15.5587 28.0611C16.4717 28.3141 17.0327 28.5011 17.0327 29.2161C17.0327 29.9311 16.4827 30.4151 15.5367 30.4151C14.5797 30

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\logo[2].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	11736
Entropy (8bit):	4.155371570154707
Encrypted:	false
SSDEEP:	192:7dH3XblyM74q2vrCWPYTanOild5wbcuS9DsTLEh4QJEOaEzt6/FM1naSHUxGB1Yk:8DeiJw4LDsUh4uIytUFE0oBkEsM
MD5:	8DCC6EE640B3A0873DB2CD12D24CE64C
SHA1:	137024194B22DE90F0DB33F9AE69D3D259BC10A4
SHA-256:	9F7EC21D7D5169533FBB0F74EA6F332AC0E8633E90B5C45AF54C8A45C5E52A70
SHA-512:	E8457B59F9E49CCA64A4B8FCB0648026C972E91E78C157B7DD63BD0BFB680F968F6BAD4DDA6A7F61CE075D17585775283DB51DF17B101A74CCE04A39AC6086A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secure.acuityscheduling.com/img/marketing/squarespace/logo.svg
Preview:	<svg width="230" height="33" viewBox="0 0 230 33" fill="none" xmlns="http://www.w3.org/2000/svg">.<path d="M0.175995 31.3941H1.46299L2.255 29.1391H5.676L6.46799 31.3941H7.832V31.0091L5.06 23.4961H2.981L0.175995 31.0091V31.3941ZM3.124 26.7081C3.498 25.6521 3.652 25.1901 3.828 24.6951H4.1689C4.32299 25.1681 4.51 25.7291 4.851 26.7081L5.27999 27.9621H2.673L3.124 26.7081Z" fill="white"/>.<path d="M12.4567 29.2711C12.7097 30.8111 13.8647 31.5701 15.4927 31.5701C17.2417 31.5701 18.4737 30.5911 18.4737 29.1171C18.4737 27.7421 17.6047 27.3021 16.1857 26.8621L15.6247 26.6861C14.7227 26.4001 14.1727 26.1911 14.1727 25.5311C14.1727 24.9481 14.6567 24.5301 15.4597 24.5301C16.3177 24.5301 16.7907 24.9151 16.9557 25.5751L18.2757 25.4651C18.1107 24.1781 17.1207 23.3421 15.5037 23.3421C13.7767 23.3421 12.6987 24.2881 12.6987 25.6081C12.6987 26.8621 13.5567 27.5001 14.9647 27.8961L15.5587 28.0611C16.4717 28.3141 17.0327 28.5011 17.0327 29.2161C17.0327 29.9311 16.4827 30.4151 15.5367 30.4151C14.5797 30

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\massage-large[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=4, xresolution=62, yresolution=70, resolutionunit=2], baseline, precision 8, 1439x719, frames 3
Category:	downloaded
Size (bytes):	123611
Entropy (8bit):	7.908670313911447
Encrypted:	false
SSDEEP:	3072:Ym/obcQ/7wPtpcnSRpP5iTV5ceM/6A0MeCWRbirFdC4:4natpcnSXwfcxLe5yT
MD5:	F357FF65FBCCB7757C40B16BF30C536C
SHA1:	5D3A1CD539BCFBEC6FBF9936C9202A7985C126CF
SHA-256:	7878A59C60ECB2D4360A02E7462213B7FF62FE9AC4C8DA69F5F295E4492EC7A4
SHA-512:	053A87974338621A48599907E452D8BCB182869852523E8AECA3B1413B7170EED99B5135ED5E617CA2FDD09D122B88F7EAC922C06A1D6F1D15DB68BD0390B77
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/massage-large.jpg
Preview:	......JFIF.....H.H.....VExif..MM.*.....>.....F.(.....H.....H.....C.....I....."$".$.....C.....G.....!1.A..Qa."q..2...B....R...#.b.3r$..%S..4Cc.5.....*.....1..!AQ."2.aBq3RC.....?.$....hO...6@.....9.TD.{..2`...J..$.@...v@.. I.(&.(.sj....."....$LH...3..@Q3q."....(.A....@.[D4L8b.PCh...5A.P....z.A6,.AH.1B...|..n.Q...Fl.Q."l....o3.).HD1Q4. ."D.=.T..p.h:`wA."...("w..QG4^...o.v(...(...1".O).p...h}vDDI.kxE@.R..r"GdR.L.....R..'..0....(.@.\N.)...&`.{ ..;D..,4.....#..i.... `E.PX.|".A..S."..I.4Zw..>@.3&.....{"..f$.=.q...Q1...P"..Q..4....V@&O5..S&....3....1....x. ....."iv.vA.-.z".....uA...3(.S..@X.I.:...&I.H..l...m....._...I.....s=.....P.3p`.....4.....Y..h.{.....A."...J!l..A.oX. ..w.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\schedule.all[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\schedule.all[1].js	
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	594016
Entropy (8bit):	5.608619736340358
Encrypted:	false
SSDEEP:	6144:NuoYOEFLbS+krkFujz31z3vJCpkhFHsiTHpKmm3y1nXe7P26cnm:m5FLhctROXyIzvKm
MD5:	AC5FC9A9B624EB8EFA652E36D0BFD596
SHA1:	226835BBD3F806F9F469903D480B2C8869F28F55
SHA-256:	6CE97B84ED65FD34D919F50E0259BDD310992DF32577C8C665179D04F2FD6D7B
SHA-512:	5847566AC24D2D8A9D738CF398A1D0DC5095A76109CAEACBFD514769F2B191B661C1B27D6D1F9866C9B3BF75548A9C666DE0139F2F7E8563CF87CEC7C14252
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/built/csp/schedule.all.js?v=c1a593
Preview:	if(function(e,t){var n,r,i=typeof t,o=e.document,a=e.location,s=e.jQuery,u=e.$,l={},c=[],p="1.9.1",f=c.concat,d=c.push,h=c.slice,g=c.indexOf,m=l.toString,y=l.hasOwnProperty,v=p.trim,b=function(e,t){return new b.fn.init(e,t,r)},x=/[+-]?(?:\d*\.|)\d+(?:[eE][+-]?\d+|)/.source,w=/\S+/g,T=/^[\s\uFEFF\xA0]+\|[\s\uFEFF\xA0]+$/g,N=/^(?:<[\w\W]+>)[^>]*|#([\w-]*))$/,C=/^<(\w+)\s*\/?>(?:<\/\1>\|)$/,k=/^[\],:{}\s]*$/,E=/(?:^|:|,)(?:\s*\[)+/g,S=/\\(?:["\\\/bfnrt]|u[\da-fA-F]{4})/g,A=/"[^"\\\r\n]*"|true|false|null|-?(?:\d+\.|)\d+(?:[eE][+-]?\d+|)/g,j=/^-ms-/,D=/-([\da-z])/gi,L=function(e,t){return t.toUpperCase()},H=function(e){(o.addEventListener||"load"===e.type||"complete"===o.readyState)&&(q(),b.ready())},q=function(){o.addEventListener?(o.removeEventListener("DOMContentLoaded",H,!1),e.removeEventListener("load",H,!1)):(o.detachEvent("onreadystatechange",H),e.detachEvent("onload",H))};function M(e){var t=e.length,n=b.type(e);return!b.isWindow(e)&&(!(1!==e.nodeType||!t)||("array"===n||"function"!=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\screen-control[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 428 x 310, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	27277
Entropy (8bit):	7.966816134401095
Encrypted:	false
SSDEEP:	768:sOIWBXEGFF3DCixZGUaGo3MoCOILEZLeR6i:2doF3DdZGUaXrCJEZLqP
MD5:	FABD57502002C19C8CE6BD1ED188B71A
SHA1:	DDFDEF47684ECE34966DAD5B958833ECB5CD3573
SHA-256:	51EA5B1C3B9F5BCDB8C8BD31146F983A3A7E2FB276668DD7ECC8179E928C8D92
SHA-512:	CFCFE7029BE0B57C2A98B1ECFC0171DDF214F3B4156A3D2F4D77A8D329265336BF9E81BAF6B7B0DDC2205076B690A9E486CEBDA229F56135B7F74161BF54BE8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/screen-control.png
Preview:	.PNG.....IHDR.....6.....=5.....gAMA.....a.... cHRM..z&.....u0...`.:....p..Q<....bKGD.....pHYs.....i.IDATx..}pT.....Rhlx...).M".(.H.p.rUVJbc../.8..W..?. ..NR....&..N.5.....Wf.....,...6.-@.["....t#..k.nE-.-...?.s.....T....v.=.|...<Gy.... ..X.<..Q%.n.A.... .".. H... ....".. ..,. .. .".. H... .... .. H... ..,. .. .".. ..,. .... .. H... ..,. .. .".. ....".. ..,. .. .".. H... ....".. ..,. .. .".. H... .... .. H... ..,. .. .".. ..V.-.w<.....A,Z~..^$&..".. ..,. .... .. H.....u...[....>.w.N._.n.UU5.d....:...e...Kv...d.:..k.s..m..-.v....q..[N.5....sfz?... u..bq.].*.(..B..(..{...P.(.TU.b.2C...P..H;...WU....+;.....F.d.(...Q_6v~..^.....~_:.N.[...Z.7.k..o.....V.RvN....oT....5.....e.".Ega.z..p..\xTU#V...._V.....KM.M.s....Xe.H..Z..U...1 ..70F..o.....4d....G.....c.s..(..5[...Y.}.d.A.y&...nt...A.zl. ....i,..n....."k@u.F`D...W..J..........r_....c.5Zv...o&.hd..5.b.eBd....dj...w.H...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\site-schooner-coaching[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	8699
Entropy (8bit):	3.9151013629292524
Encrypted:	false
SSDEEP:	192:niy8nXw7U9ZNwJ2/M9V+0347iXAlaveVJmP1dXZ:7YXfBy+0ol0BZ
MD5:	1804EDAA825DFC5A13A7C4943C8521F9
SHA1:	FB6E2D049D06B58F08C99A49E2079CFA6D34FF55
SHA-256:	C6C27EF02E80F44FA280699E3A178FDFC17738BFEDAF669EBB49570BB9593035
SHA-512:	363C161D98C2B9DA22FDC6C9A91EEC643D44BBA05CBC60F90B359A5D4287EC3DC4DADBA3C58B7A764A36074D9E6D31DCE144CC4751E5B82E8CC19480F2F426F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/site-schooner-coaching.svg
Preview:	<svg width="475" height="340" xmlns="http://www.w3.org/2000/svg"><g fill="none" fill-rule="evenodd"><path fill="#BBC2CA" d="M0 0h475v340H0z"/><g fill="#FFF" fill-rule="nonzero"><path d="M110.768 189.54a5.357 5.357 0 0 0-2.422-1.85c-.996-.39-1.97-.584-2.92-.584-1.217 0-2.323.222-3.319.667a7.779 7.779 0 0 0-2.572 1.834 8.158 8.158 0 0 0-1.66 2.735c-.386 1.045-.58 2.18-.58 3.402 0 1.29.188 2.468.564 3.535.376 1.068.913 1.985 1.61 2.752a7.231 7.231 0 0 0 2.505 1.784c.974.423 2.069.634 3.286.634 1.26 0 2.378-.25 3.351-.75.974-.5 1.76-1.162 2.356-1.985l3.352 2.368a10.748 10.748 0 0 1-3.816 3.052c-1.505.723-3.263 1.084-5.277 1.084-1.836 0-3.523-.306-5.06-.917-1.538-.612-2.86-1.468-3.966-2.568-1.106-1.101-1.969-2.413-2.588-3.936-.62-1.523-.93-3.207-.93-5.053 0-1.89.327-3.597.98-5.12.652-1.523 1.548-2.818 2.687-3.885 1.14-1.068 2.484-1.89 4.032-2.468 1.549-.579 3.23-.868 5.044-.868.753 0 1.538.073 2.357.217a11.94 11.94 0 0 1 2.356.667c.752.3 1.46.673 2.124 1.118a6.85 6.85 0 0 1 1.692 1.6l-3.186

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\site-under-pressure[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	15579
Entropy (8bit):	3.8639968435948133
Encrypted:	false
SSDEEP:	384:Zy4uUs7bgY2W5ILHFkz9kqJTeoG0eHD9reo:U4uUM22ILHFoTJqD0MDoo
MD5:	EAAF1195AA71A574FEA61EDE7128CC69
SHA1:	D24B8E6DADBF42EC410FCBC2FC1112513DF6442A
SHA-256:	D8F317161A53DA0E71D6D028471D5759617274FCCF8B8CCF7F18220D14928064
SHA-512:	E84ED8FFB4F3DC992D4DE368E00F60AE335AABDCC144A2114B7C366A4456E9B78CF2ACC507B40C52F4017CE6A94992AEB111CAA2FA1B5F5E664E1EC262C3B000
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/site-under-pressure.svg
Preview:	<svg width="475" height="340" xmlns="http://www.w3.org/2000/svg"><g fill="none" fill-rule="evenodd"><path fill="#CABBC8" d="M0 0h475v340H0z"/><path stroke="#FFF" stroke-width="1.768" opacity=".595" d="M77.884 119.879h318.232V220.12H77.884z"/><path d="M92.908 182.88h4.085l1.982 7.947c.21.882.375 1.721.496 2.51 9.12.797.237 1.548.35 2.254h.097c.113-.706.23-1.457.35-2.254.121-.798.286-1.637.496-2.52l2.042-7.945h4v20.533h-2.924v-6.793a143.698 143.698 0 0 1 .109-5.656 85.92 85.92 0 0 1 .108-2.134c.04-.617.077-1.106.11-1.466h-.23l-3.119 13.404h-1.982l-3.142-13.404h-.23c.033.36.069.85.11 1.466.04.617.076 1.329.108 2.134a140.027 140.027 0 0 1 .109 5.656v6.793h-2.925V182.88zm31.191 0h3.602l3.819 20.534h-3.166l-.568-3.679h-3.771l-.544 3.679h-3.179l3.807-20.533zm3.324 14.51l-1.45-10.23h-.133l-1.463 10.23h3.046zm16.785 1.864c0-.44.026-.847.079-1.22.052-.373.13-.775.235-1.208h2.43v.998c0 .553.034 1.042.102 1.466.069.425.182.784.339 1.076.157.293.366.513.628.661.262.149.582.223.961.223.596 0 1.051-.1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\support[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=4, xresolution=62, yresolution=70, resolutionunit=2], progressive, precision 8, 583x695, frames 3
Category:	downloaded
Size (bytes):	134479
Entropy (8bit):	7.982949655710601
Encrypted:	false
SSDEEP:	3072:Z9dldQHc1nB9xYJLzXF0pNm9ZBvuT//iHIpqM2VuU:LdQHcdju5zXl9Pc//iST24U
MD5:	2BC931CE12885842F2CB215A16CF1C12
SHA1:	BFF81BDD37BA0FCEB28180BAB860B8FFDD64A15B
SHA-256:	6FFA4B5B9CEC59633E64B6F4057729E5CED6B9CC57C9C6B8BC5DF255FB8B5CA2
SHA-512:	32AA657EB3A9CB959CAD1780D9B277F4F8AE678B2120830EE627E56F1A5D416802A7327B826760003CFE626A54DD5B8669DC790B9E22CD4E759184E6C07CEE4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn-marketing.acuityscheduling.com/img/marketing/squarespace/v3/support.jpg
Preview:	......JFIF.....H.H.....VExif..MM.*.....>.....F.(.....H.....H.....*.....*.....G..".....C.O.@W)..sD...f..ho..Gl.....s.I.....n...a..c....2..cd..V...!]1!.&...HV.J.g.....J=...(@....5..."....I.?#..-..U....x.C,.No.s.{.g.>R.I.F.....l..P ...X.f.Pe... ...).9....Y4.3...[.s.@j.W..M.cQ.V..$n....e.w..i.....Xb.....Z....v%R.!"...A.....sO...i(....M.%O..G..6...~...O`.z!.....P./.M...(..%.m..y...R.h..XK....K..qAe;.....C.Qx..1f..yP .....m.....z..pb...C.J...Tu.8..B.P).....(.7...Oe..).v^"...&.ma..DcP.....t.m.'us...b3z.-.8..2...9...0.'.4..?0K..w;b....f'<#>F.....W.-.c.....]q..vq.y..z..Ek...d..ffo."D.s.m.+7.....A.... ~H...T..%.HvK.hu6....::..o..\....G...:Y.....S..)..e.....2V.N.l.a.X>.B.G...s..1.i$.P.....L....Z...soEd#l:.S....

C:\Users\user\AppData\Local\Temp\~DF1208AB93F940F0FF.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	80165
Entropy (8bit):	1.7045772737433464
Encrypted:	false
SSDEEP:	1536:a48Db1EoDKSJUeLJ/+gUeLJ/3cgUeLJ/nqfcemqCemqT:a48Db1EoDKSJUeLJ/+gUeLJ/sgUeLJ/A
MD5:	44FB647990AAB31C924C35A2CA6F65C8
SHA1:	8B4263E0060794B7DB8A6E670142038F5640DF3F
SHA-256:	47E3733BA699C35579D217FE2F4AE570B9395B150C4EB00133783B1F4AE8CF9B
SHA-512:	0EA95FC0B364F55767C3DF7AEC0D6045E0332CCC813351BE380FBC1E9389B2E4F42B29B80839CD2B7F8117A174FE81D74872209754CBD4091CD03DE584D8ECC
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF26AA1685C1C23235.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Temp\~DF26AA1685C1C23235.TMP	
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.34683085753494797
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAgg9G:kBqoxxJhHWSVSEab
MD5:	B1624E2E2EFB55CDCA505400071D8A88
SHA1:	A79FBD6FB13ECE44B85BBF42C256DF8F5E924238
SHA-256:	75C86824B3B6B699EC5EF82FED781CC04BA5C23A40E8B97E5B076750C290C603
SHA-512:	30E0A54562D30A6915AF0389B8EE331E361292FBBD750A9E6A4E667D2F8E8C19396AB14D8587B0961484A3D0C9E68767891D94ED16C64A897B6ACA8CBD46C9E
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF904815EF7ED92817.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	50571
Entropy (8bit):	0.28825402127537947
Encrypted:	false
SSDEEP:	48:kBqoxxJhHWSVSEabOeud2P282e2Dh2CDaBDK:kBqoxDhHWSVSE+OeudWV/6h1J
MD5:	FEBE5281508DD01B6DDB016E9CBD9B67
SHA1:	7BFC7CC6A1D70F54FF43E1F0A71F255343B1FF87
SHA-256:	A7E11C968DAC16828A55827A269D76BB32D1DF10E5856798A2A6D6A95682A09A
SHA-512:	7574F9B852CA813F80A24468BFB58C6FB94D78643E0FD4A06A7B66DDBC72D00A9823C6F24092DC2F4CB764310B3109443423F5B999B74254F3E2A0B054BDEB9E
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

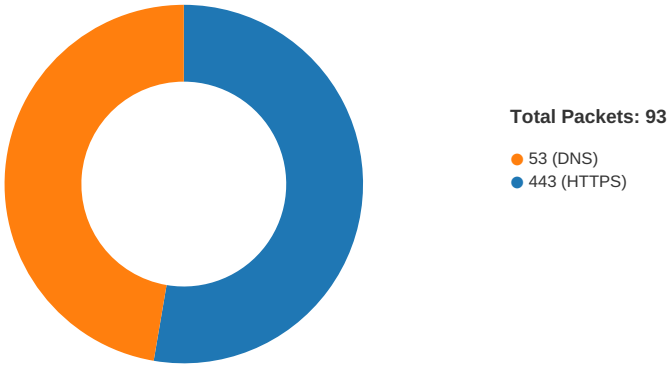
C:\Users\user\AppData\Local\Temp\~DFF5C0B19FBFB1A0C0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13125
Entropy (8bit):	0.5490494637711433
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loRF9loz9lWOyZ8l8bGdS:kBqol0qOa8W
MD5:	E8D353F9D84843EAF7581CE6D43C7238
SHA1:	2B1C2AFFAF93231A8AFE0A3960D287EDC6690D1C
SHA-256:	565DC22396BA0DD618367F851FD621AAEC1C0D317D00295F39F41E869DF81CF9
SHA-512:	883157B0361A591068E1E10132513BE3D3C1077D92787F27FAC7F94404A01120DC863B696AA2E00FF60B1F2F2A346B9555086188DE179FF4822B20D0C3645800
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
Mar 15, 2021 17:35:09.659950972 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:09.660439014 CET	49716	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:09.866374016 CET	443	49716	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:09.866476059 CET	49716	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:09.866862059 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:09.866949081 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:09.871841908 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:09.871891022 CET	49716	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.079237938 CET	443	49716	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.079832077 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.079893112 CET	443	49716	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.079909086 CET	443	49716	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.079937935 CET	443	49716	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.079957008 CET	443	49716	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.079974890 CET	443	49716	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.080005884 CET	49716	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.080127954 CET	49716	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.080575943 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.080595970 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.080620050 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.080640078 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.080650091 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.080679893 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.080795050 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.123631001 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.123716116 CET	49716	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.131527901 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.131643057 CET	49716	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.131866932 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.332427025 CET	443	49716	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.332494020 CET	443	49716	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.332508087 CET	49716	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.332561016 CET	49716	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.333141088 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.333185911 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.333241940 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.333281040 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.333328962 CET	49716	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.333822012 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.339852095 CET	443	49716	35.160.170.4	192.168.2.3

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 15, 2021 17:35:10.339966059 CET	49716	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.340522051 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.340610027 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.383222103 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.416425943 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.416651964 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.424088955 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.424163103 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.424223900 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.424237013 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.424261093 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.424278975 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.424285889 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.424335957 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.424377918 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.424405098 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.504508018 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.540256977 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.581381083 CET	443	49716	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.711404085 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.716747999 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.716840029 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.716872931 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.716895103 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:10.716895103 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:10.716944933 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:11.255935907 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:11.457067966 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:11.462059975 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:11.462167978 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:11.503029108 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:11.665874958 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:11.670794010 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:11.670830011 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:11.671231985 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:11.671264887 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:11.671288013 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:11.671338081 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:11.671365023 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:11.703725100 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:11.703768015 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:11.703811884 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:11.703840017 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:29.428385019 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:29.679138899 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:29.682230949 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:29.682379961 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:29.688873053 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:29.688939095 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:29.688997984 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:29.689058065 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:29.689112902 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:29.689117908 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:29.689162016 CET	443	49715	35.160.170.4	192.168.2.3
Mar 15, 2021 17:35:29.689218998 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:29.689271927 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:29.928039074 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:29.985142946 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:29.986766100 CET	49715	443	192.168.2.3	35.160.170.4
Mar 15, 2021 17:35:30.134711981 CET	443	49715	35.160.170.4	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 15, 2021 17:35:00.787189007 CET	50620	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:00.849967003 CET	53	50620	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:01.203977108 CET	64938	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:01.255475998 CET	53	64938	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:02.378833055 CET	60152	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:02.430249929 CET	53	60152	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:03.537609100 CET	57544	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:03.589148045 CET	53	57544	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:05.063251972 CET	55984	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:05.120632887 CET	53	55984	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:07.427902937 CET	64185	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:07.477495909 CET	53	64185	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:08.522447109 CET	65110	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:08.582298040 CET	53	65110	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:08.761265039 CET	58361	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:08.815229893 CET	53	58361	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:09.576682091 CET	63492	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:09.641518116 CET	53	63492	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:10.477472067 CET	60831	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:10.515152931 CET	60100	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:10.535734892 CET	53	60831	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:10.583230019 CET	53	60100	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:10.878181934 CET	53195	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:10.944242954 CET	53	53195	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:12.429970026 CET	50141	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:12.481648922 CET	53	50141	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:13.572994947 CET	53023	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:13.626362085 CET	53	53023	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:14.754586935 CET	49563	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:14.803260088 CET	53	49563	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:16.224622011 CET	51352	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:16.284508944 CET	53	51352	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:17.492607117 CET	59349	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:17.544356108 CET	53	59349	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:18.703155041 CET	57084	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:18.752259016 CET	53	57084	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:19.870903015 CET	58823	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:19.923060894 CET	53	58823	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:21.013439894 CET	57568	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:21.065697908 CET	53	57568	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:22.217277050 CET	50540	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:22.274719000 CET	53	50540	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:23.294620037 CET	54366	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:23.346188068 CET	53	54366	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:26.053742886 CET	53034	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:26.111264944 CET	53	53034	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:26.624444008 CET	57762	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:26.673491955 CET	53	57762	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:33.663249969 CET	55435	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:33.722718954 CET	53	55435	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:34.536225080 CET	50713	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:34.596295118 CET	53	50713	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:34.711074114 CET	56132	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:34.770822048 CET	53	56132	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:34.864387035 CET	58987	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:34.866059065 CET	56579	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:34.888365030 CET	60633	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:34.918544054 CET	53	56579	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:34.925455093 CET	53	58987	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:34.956136942 CET	53	60633	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:35.282006025 CET	61292	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:35.332571030 CET	53	61292	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:35.675091982 CET	63619	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:35.734085083 CET	53	63619	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 15, 2021 17:35:38.520335913 CET	64938	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:38.573012114 CET	53	64938	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:39.146013021 CET	61946	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:39.197443008 CET	53	61946	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:39.414251089 CET	64910	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:39.465976954 CET	53	64910	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:39.512347937 CET	64938	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:39.565860987 CET	53	64938	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:39.816658974 CET	52123	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:39.877274990 CET	53	52123	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:40.145761013 CET	61946	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:40.198899031 CET	53	61946	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:40.527334929 CET	64938	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:40.578938007 CET	53	64938	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:41.316787958 CET	61946	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:41.368350029 CET	53	61946	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:42.536293983 CET	64938	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:42.588130951 CET	53	64938	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:43.317358971 CET	61946	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:43.369141102 CET	53	61946	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:46.552412987 CET	64938	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:46.604028940 CET	53	64938	8.8.8.8	192.168.2.3
Mar 15, 2021 17:35:47.333374977 CET	61946	53	192.168.2.3	8.8.8.8
Mar 15, 2021 17:35:47.385135889 CET	53	61946	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 15, 2021 17:35:09.576682091 CET	192.168.2.3	8.8.8.8	0xacf6	Standard query (0)	ph-northwestmi.as.me	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:10.477472067 CET	192.168.2.3	8.8.8.8	0x260e	Standard query (0)	cdn-marketing.acuityscheduling.com	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:26.053742886 CET	192.168.2.3	8.8.8.8	0x6466	Standard query (0)	favicon.ico	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:33.663249969 CET	192.168.2.3	8.8.8.8	0x7f7b	Standard query (0)	www.acuityscheduling.com	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:34.536225080 CET	192.168.2.3	8.8.8.8	0x4fcd	Standard query (0)	consent.trustarc.com	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:34.866059065 CET	192.168.2.3	8.8.8.8	0xd859	Standard query (0)	dev.visualwebsiteoptimizer.com	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:34.888365030 CET	192.168.2.3	8.8.8.8	0x2474	Standard query (0)	cdn.amplitude.com	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:35.282006025 CET	192.168.2.3	8.8.8.8	0x2d1f	Standard query (0)	api.amplitude.com	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:35.675091982 CET	192.168.2.3	8.8.8.8	0x19c8	Standard query (0)	secure.acuityscheduling.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 15, 2021 17:35:09.641518116 CET	8.8.8.8	192.168.2.3	0xacf6	No error (0)	ph-northwestmi.as.me		35.160.170.4	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:09.641518116 CET	8.8.8.8	192.168.2.3	0xacf6	No error (0)	ph-northwestmi.as.me		52.89.211.128	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:10.535734892 CET	8.8.8.8	192.168.2.3	0x260e	No error (0)	cdn-marketing.acuityscheduling.com	i3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Mar 15, 2021 17:35:26.111264944 CET	8.8.8.8	192.168.2.3	0x6466	Name error (3)	favicon.ico	none	none	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:33.722718954 CET	8.8.8.8	192.168.2.3	0x7f7b	No error (0)	www.acuityscheduling.com		35.160.170.4	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:33.722718954 CET	8.8.8.8	192.168.2.3	0x7f7b	No error (0)	www.acuityscheduling.com		52.89.211.128	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 15, 2021 17:35:34.596295118 CET	8.8.8.8	192.168.2.3	0x4fcd	No error (0)	consent.trustarc.com		13.224.94.16	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:34.596295118 CET	8.8.8.8	192.168.2.3	0x4fcd	No error (0)	consent.trustarc.com		13.224.94.3	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:34.596295118 CET	8.8.8.8	192.168.2.3	0x4fcd	No error (0)	consent.trustarc.com		13.224.94.13	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:34.596295118 CET	8.8.8.8	192.168.2.3	0x4fcd	No error (0)	consent.trustarc.com		13.224.94.105	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:34.918544054 CET	8.8.8.8	192.168.2.3	0xd859	No error (0)	dev.visualwebsiteoptimizer.com		34.96.102.137	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:34.956136942 CET	8.8.8.8	192.168.2.3	0x2474	No error (0)	cdn.amplitude.com		13.224.89.109	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:34.956136942 CET	8.8.8.8	192.168.2.3	0x2474	No error (0)	cdn.amplitude.com		13.224.89.45	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:34.956136942 CET	8.8.8.8	192.168.2.3	0x2474	No error (0)	cdn.amplitude.com		13.224.89.35	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:34.956136942 CET	8.8.8.8	192.168.2.3	0x2474	No error (0)	cdn.amplitude.com		13.224.89.71	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:35.332571030 CET	8.8.8.8	192.168.2.3	0x2d1f	No error (0)	api.amplitude.com		54.184.84.60	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:35.332571030 CET	8.8.8.8	192.168.2.3	0x2d1f	No error (0)	api.amplitude.com		52.41.34.182	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:35.332571030 CET	8.8.8.8	192.168.2.3	0x2d1f	No error (0)	api.amplitude.com		54.71.99.68	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:35.332571030 CET	8.8.8.8	192.168.2.3	0x2d1f	No error (0)	api.amplitude.com		44.241.86.255	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:35.332571030 CET	8.8.8.8	192.168.2.3	0x2d1f	No error (0)	api.amplitude.com		44.225.30.99	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:35.332571030 CET	8.8.8.8	192.168.2.3	0x2d1f	No error (0)	api.amplitude.com		35.155.144.10	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:35.332571030 CET	8.8.8.8	192.168.2.3	0x2d1f	No error (0)	api.amplitude.com		50.112.24.180	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:35.332571030 CET	8.8.8.8	192.168.2.3	0x2d1f	No error (0)	api.amplitude.com		52.25.136.101	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:35.734085083 CET	8.8.8.8	192.168.2.3	0x19c8	No error (0)	secure.acityscheduling.com		52.89.211.128	A (IP address)	IN (0x0001)
Mar 15, 2021 17:35:35.734085083 CET	8.8.8.8	192.168.2.3	0x19c8	No error (0)	secure.acityscheduling.com		35.160.170.4	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 15, 2021 17:35:10.079957008 CET	35.160.170.4	443	192.168.2.3	49716	CN=acuityscheduling.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sun Sep 13 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Wed Oct 13 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Mar 15, 2021 17:35:10.080640078 CET	35.160.170.4	443	192.168.2.3	49715	CN=acuityscheduling.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sun Sep 13 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Wed Oct 13 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 15, 2021 17:35:34.139050961 CET	35.160.170.4	443	192.168.2.3	49734	CN=acuityscheduling.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sun Sep 13 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Wed Oct 13 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Mar 15, 2021 17:35:34.140829086 CET	35.160.170.4	443	192.168.2.3	49735	CN=acuityscheduling.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sun Sep 13 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Wed Oct 13 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 15, 2021 17:35:34.732536077 CET	13.224.94.16	443	192.168.2.3	49736	CN=*.trustarc.com, O=TrustArc Inc, L=San Francisco, ST=California, C=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu May 21 19:53:46 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Jul 17 21:03:01 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Mar 15, 2021 17:35:34.744885921 CET	13.224.94.16	443	192.168.2.3	49737	CN=*.trustarc.com, O=TrustArc Inc, L=San Francisco, ST=California, C=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu May 21 19:53:46 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Jul 17 21:03:01 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 15, 2021 17:35:35.008383036 CET	34.96.102.137	443	192.168.2.3	49740	CN=*.visualwebsiteoptimizer.com, OU=Domain Control Validated CN=Starfield Secure Certificate Authority - G2, OU=http://certs.starfieldtech.com/repository/, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Starfield Secure Certificate Authority - G2, OU=http://certs.starfieldtech.com/repository/, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sat Jun 20 00:03:14 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014	Wed Jul 06 14:37:36 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031	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=Starfield Secure Certificate Authority - G2, OU=http://certs.starfieldtech.com/repository/, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
Mar 15, 2021 17:35:35.010565996 CET	34.96.102.137	443	192.168.2.3	49741	CN=*.visualwebsiteoptimizer.com, OU=Domain Control Validated CN=Starfield Secure Certificate Authority - G2, OU=http://certs.starfieldtech.com/repository/, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Starfield Secure Certificate Authority - G2, OU=http://certs.starfieldtech.com/repository/, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sat Jun 20 00:03:14 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014	Wed Jul 06 14:37:36 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031	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=Starfield Secure Certificate Authority - G2, OU=http://certs.starfieldtech.com/repository/, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
Mar 15, 2021 17:35:35.100765944 CET	13.224.89.109	443	192.168.2.3	49744	CN=cdn.amplitude.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Nov 18 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Dec 18 00:59:59 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Mar 15, 2021 17:35:35.115056038 CET	13.224.89.109	443	192.168.2.3	49745	CN=cdn.amplitude.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Nov 18 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Dec 18 00:59:59 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Mar 15, 2021 17:35:35.755438089 CET	54.184.84.60	443	192.168.2.3	49746	CN=*.amplitude.com CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Feb 18 01:00:00 CET 2020 Wed Feb 12 01:00:00 CET 2014 Thu Jan 01 01:00:00 CET 2004	Mon Feb 14 00:59:59 CET 2022 Mon Feb 12 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Feb 12 01:00:00 CET 2014	Mon Feb 12 00:59:59 CET 2029		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 15, 2021 17:35:35.756669998 CET	54.184.84.60	443	192.168.2.3	49747	CN=*.amplitude.com CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Feb 18 01:00:00 CET 2020 Wed Feb 12 01:00:00 CET 2014 Thu Jan 01 01:00:00 CET 2004	Mon Feb 14 00:59:59 CET 2022 Mon Feb 12 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Feb 12 01:00:00 CET 2014	Mon Feb 12 00:59:59 CET 2029		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Mar 15, 2021 17:35:36.155486107 CET	52.89.211.128	443	192.168.2.3	49748	CN=acuityscheduling.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sun Sep 13 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Wed Oct 13 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Mar 15, 2021 17:35:36.156416893 CET	52.89.211.128	443	192.168.2.3	49749	CN=acuityscheduling.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sun Sep 13 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Wed Oct 13 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5408 Parent PID: 792

General

Start time:	17:35:06
Start date:	15/03/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff611e30000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

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: 5608 Parent PID: 5408

General

Start time:	17:35:07
Start date:	15/03/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5408 CREDAT:17410 /prefetch:2
Imagebase:	0x2d0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
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