

ID: 339434
Cookbook: browseurl.jbs
Time: 02:38:35
Date: 14/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report https://bgcaustralia.typeform.com/to/EGtXBKAf 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Dropped Files 4
Sigma Overview 4
Signature Overview 4
AV Detection: 5
Phishing: 5
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 9
URLs from Memory and Binaries 9
Contacted IPs 10
Public 11
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASN 12
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 23
No static file info 23
Network Behavior 23
Network Port Distribution 23
TCP Packets 23
UDP Packets 25
DNS Queries 26
DNS Answers 27
HTTPS Packets 28
Code Manipulations 36
Statistics 36
Behavior 36
System Behavior 36
Analysis Process: iexplore.exe PID: 6912 Parent PID: 800 36

Copyright null 2021

General 36
File Activities 36
Registry Activities 37
Analysis Process: iexplore.exe PID: 6956 Parent PID: 6912 37
General 37
File Activities 37
Registry Activities 37
Disassembly 37

Copyright null 2021

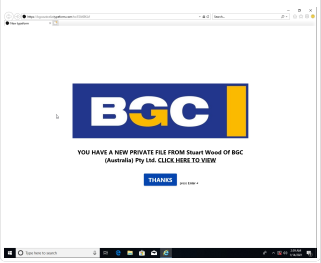
Analysis Report https://bgcaustralia.typeform.com/to/E…

Overview

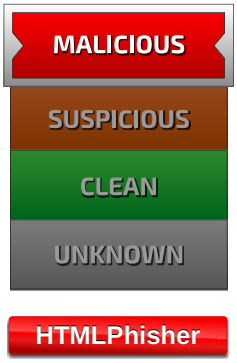
General Information

Sample URL:	http://https://bgcaustralia.typeform.com/to/EGtXBKAf
Analysis ID:	339434

Most interesting Screenshot:



Detection

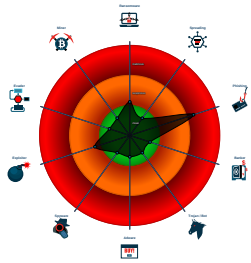


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Yara detected HtmlPhish_10
- Allocates a big amount of memory (p…
- HTML body contains low number of …
- HTML title does not match URL
- Invalid 'forgot password' link found

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6912 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6956 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6912 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

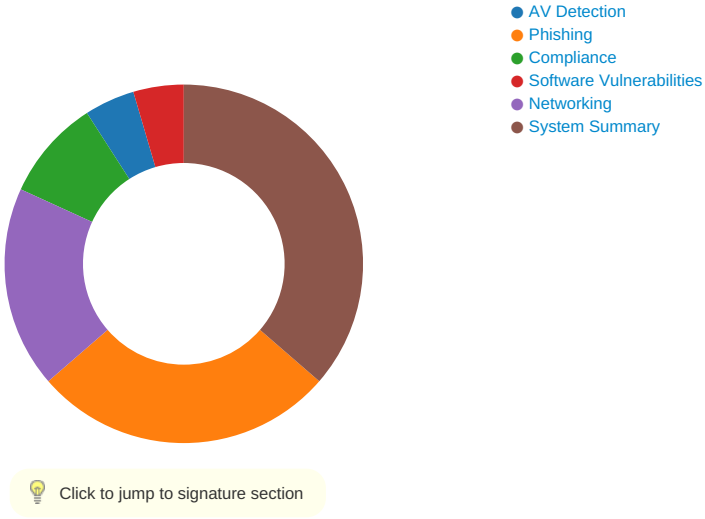
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Secure[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Phishing:

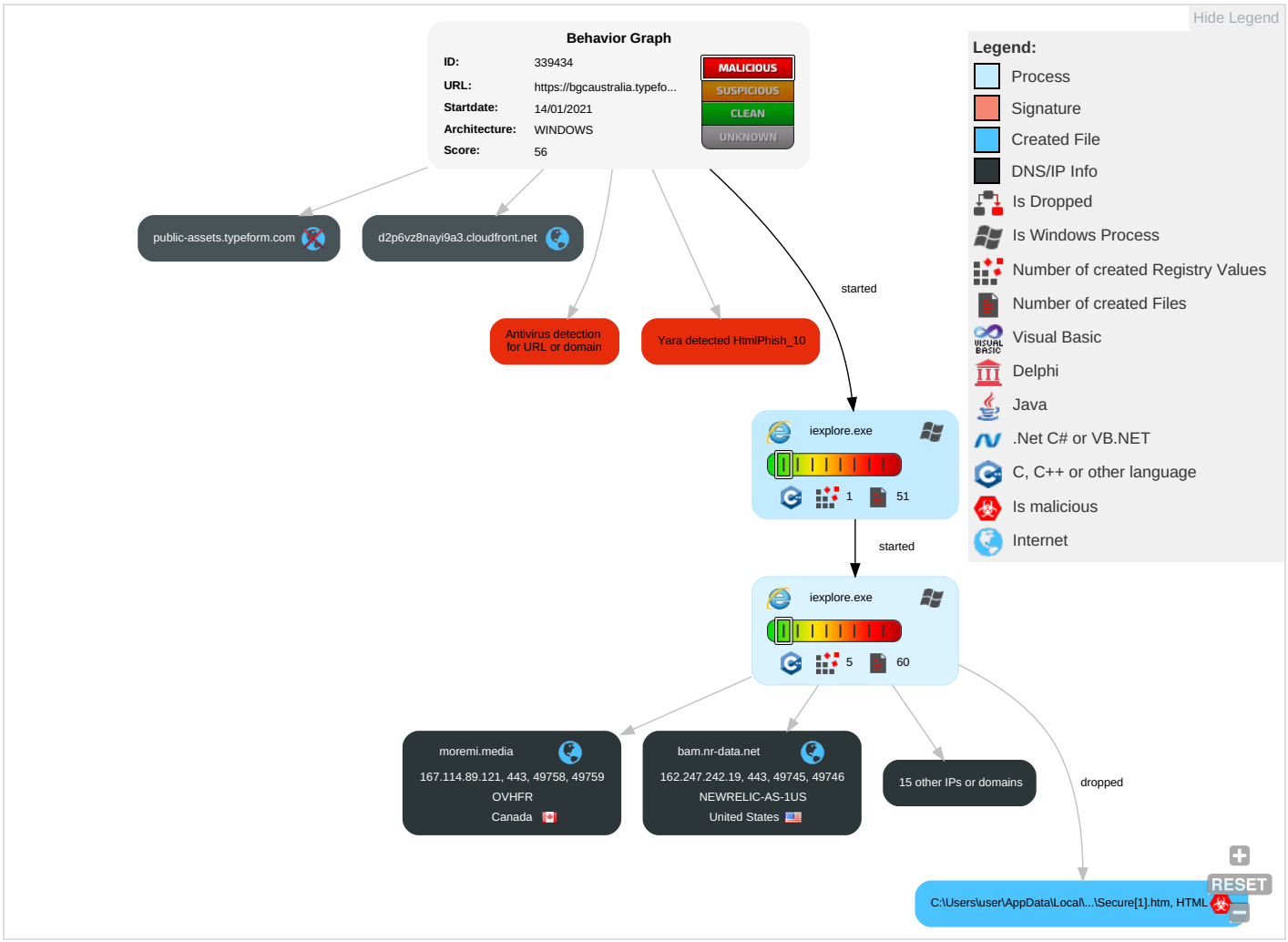
Yara detected HtmlPhish_10

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	Modify Syste Partiti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	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 Locko
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Extra Window Memory Injection 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	Delete Devic Data

Behavior Graph

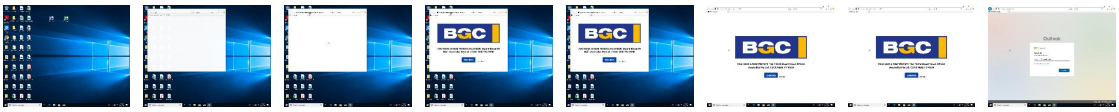
Copyright null 2021

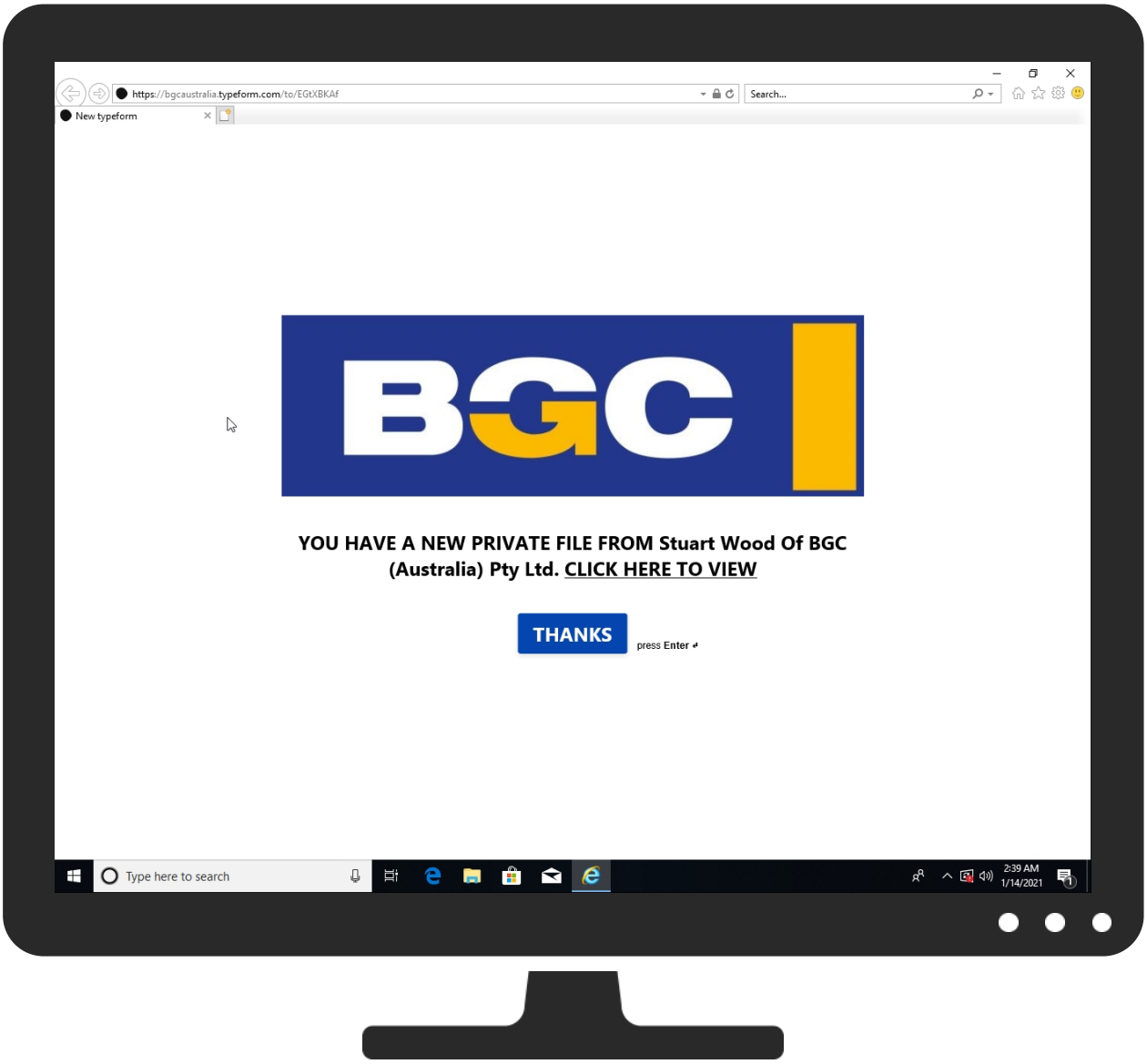


Screenshots

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://bgcaustralia.typeform.com/to/EGtXBKAf	0%	Virustotal		Browse
http://https://bgcaustralia.typeform.com/to/EGtXBKAf	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cs1100.wpc.omegacdn.net	0%	Virustotal		Browse
bam.nr-data.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link

Copyright null 2021

Source	Detection	Scanner	Label	Link
http://https://moremi.media/Secure/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_more_7568a43cf440757c55d2e7f51557ae1f.svg	0%	Avira URL Cloud	safe	
http://https://moremi.media/Secure/com/to/EGtXBKAf	100%	Avira URL Cloud	phishing	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.s	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_635a63d500a92a0b8497cdc58d0f66b1.svg	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_account_aad_9de70d1c5191d1852a0d5aac28b44	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg	0%	Avira URL Cloud	safe	
http://https://moremi.media/Secure/$Sign	100%	Avira URL Cloud	phishing	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_96f69d0cefd8a8ba623a182c351ccc64.png	0%	Avira URL Cloud	safe	
http://https://moremi.media/S	100%	Avira URL Cloud	phishing	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/applogos/53_8b36337037cff88c3df203bb73d58e41.png	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~(	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~(	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~(	0%	URL Reputation	safe	
http://https://moremi.media/Secure/#com/to/EGtXBKAf.ico	100%	Avira URL Cloud	phishing	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c.s	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_account_add_56e73414003cdb676008ff7857343	0%	Avira URL Cloud	safe	
http://https://moremi.media/Sypeform.com/to/EGtXBKAf	100%	Avira URL Cloud	phishing	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_grey_5bc252567ef56db648207d9c36a9d004.p	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
d296je7bbdd650.cloudfront.net	13.224.100.80	true	false		high
cs1100.wpc.omegacdn.net	152.199.23.37	true	false	• 0%, Virustotal, Browse	unknown
cdnjs.cloudflare.com	104.16.18.94	true	false		high
api.segment.io	52.41.92.51	true	false		high
moremi.media	167.114.89.121	true	false		unknown
d2citsn5wf4j9j.cloudfront.net	13.224.94.31	true	false		high
d2nvsmtq2poimt.cloudfront.net	13.224.94.88	true	false		high
bam.nr-data.net	162.247.242.19	true	false	• 0%, Virustotal, Browse	unknown
d2p6vz8nayi9a3.cloudfront.net	13.224.94.86	true	false		high
cdn.segment.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
bgcaustralia.typeform.com	unknown	unknown	false		high
renderer-assets.typeform.com	unknown	unknown	false		high
public-assets.typeform.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
js-agent.newrelic.com	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false		unknown
images.typeform.com	unknown	unknown	false		high

Contacted URLs

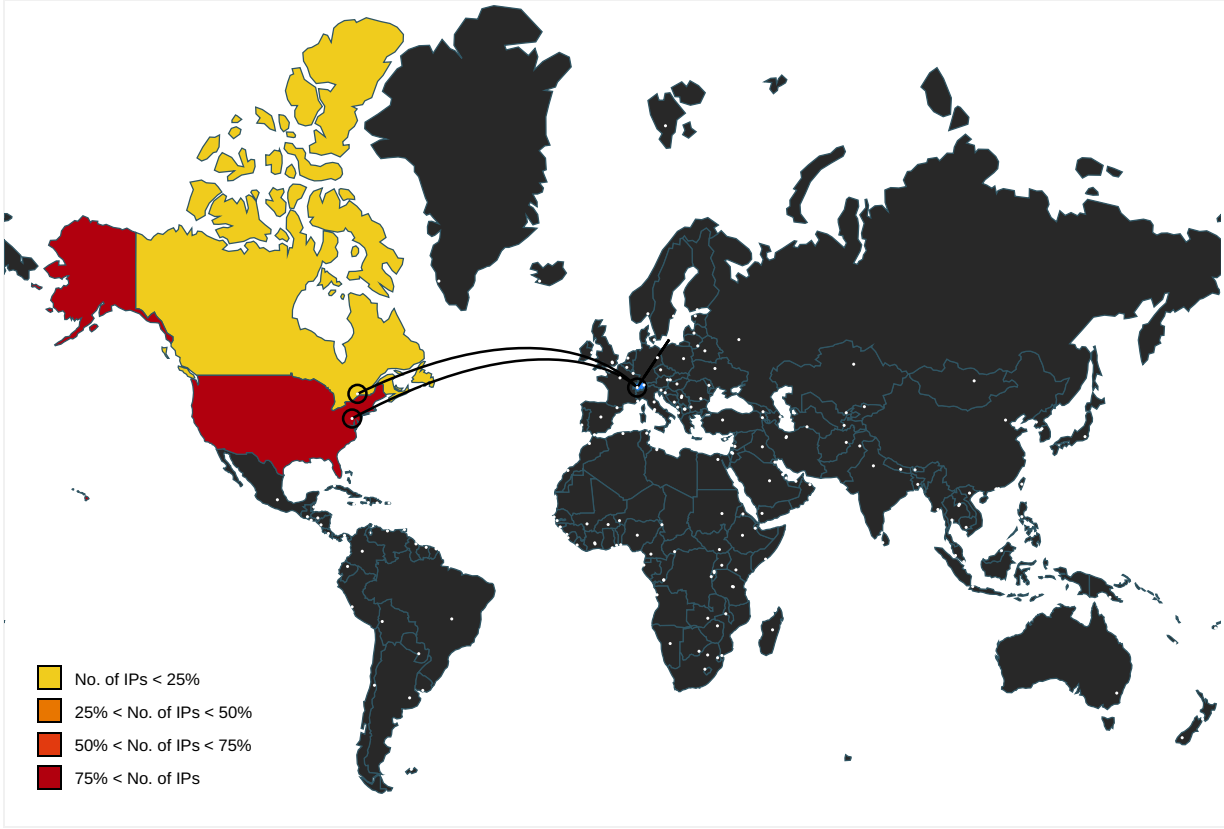
Name	Malicious	Antivirus Detection	Reputation
http://https://moremi.media/Secure/	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://bgcaustralia.typeform.com/to/EGtXBKAf	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://public-assets.typeform.com/public/favicon/favicon-32x32.png	~DF17EE954C7F130427.TMP.1.dr, EGtXBKAf[1].htm.2.dr	false		high
http://fontawesome.io	font-awesome[1].css.2.dr	false		high
http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_more_7568a43cf440757c55d2e7f51557ae1f.svg	Secure[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://moremi.media/Secure/com/to/EGtXBKAf	~DF17EE954C7F130427.TMP.1.dr	true	• Avira URL Cloud: phishing	unknown
http://https://renderer-assets.typeform.com/vendors~blocks-ranking.f8aee16223a106724ea1.js	EGtXBKAf[1].htm.2.dr	false		high
http://https://renderer-assets.typeform.com/vendors~phonenumber.32d788474b661d4d3074.js	EGtXBKAf[1].htm.2.dr	false		high
http://https://renderer-assets.typeform.com/blocks-matrix.0544beec0e1a4e11a24a.js	EGtXBKAf[1].htm.2.dr	false		high
http://https://public-assets.typeform.com/public/favicon/favicon-16x16.png	EGtXBKAf[1].htm.2.dr	false		high
http://https://aadcdn.msftauth.net/ests/2.1/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.s	Secure[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://renderer-assets.typeform.com/phonenumber.6ea5ec50b9fa21e816ff.js	EGtXBKAf[1].htm.2.dr	false		high
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_635a63d500a92a0b8497cdc58d0f66b1.svg	Secure[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bgcaustralia.typeform.com/oembed?url=https%3A%2F%2Fbgcaustralia.typeform.com%2Fto%2FEGtXBKAf	EGtXBKAf[1].htm.2.dr	false		high
http://https://github.com/kof/animationFrame	vendors~form.965f5dedbb854e83c6c8[1].js.2.dr	false		high
http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_account_aad_9de70d1c5191d1852a0d5aac28b44	Secure[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://public-assets.typeform.com/public/favicon/browserconfig.xml	EGtXBKAf[1].htm.2.dr	false		high
http://https://public-assets.typeform.com/public/favicon/site.webmanifest	EGtXBKAf[1].htm.2.dr	false		high
http://https://aadcdn.msftauth.net/ests/2.1/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg	Secure[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://public-assets.typeform.com/public/favicon/apple-touch-icon.png	EGtXBKAf[1].htm.2.dr	false		high
http://https://moremi.media/Secure/$Sign	~DF17EE954C7F130427.TMP.1.dr	true	• Avira URL Cloud: phishing	unknown
http://www.jacklmoore.com/autosize	vendors~form.965f5dedbb854e83c6c8[1].js.2.dr	false		high
http://https://bgcaustralia.typeform.com/to/EGtXBKAfRoot	{51C83D51-5609-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false		high
http://https://aadcdn.msftauth.net/ests/2.1/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.	Secure[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_96f69d0cefd8a8ba623a182c351ccc64.png	Secure[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://moremi.media/S	{51C83D51-5609-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: phishing	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/images/applogos/53_8b36337037cff88c3df203bb73d58e41.png	Secure[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://renderer-assets.typeform.com/	EGtXBKAf[1].htm.2.dr	false		high
http://www.apache.org/licenses/LICENSE-2.0	vendors~form.965f5dedbb854e83c6c8[1].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://public-assets.typeform.com/public/favicon/safari-pinned-tab.svg	EGtXBKAf[1].htm.2.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css	Secure[1].htm.2.dr	false		high
http://https://bgcaustralia.typeform.com/to/EGtXBKAf	EGtXBKAf[1].htm.2.dr	false		high
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	imagestore.dat.2.dr, Secure[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://code.jquery.com/jquery-3.1.1.min.js	Secure[1].htm.2.dr	false		high
http://https://moremi.media/Secure/	~DF17EE954C7F130427.TMP.1.dr	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~	imagestore.dat.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://renderer-assets.typeform.com/renderer.0f5a683b381b67dbbf89.js	EGtXBKAf[1].htm.2.dr	false		high
http://https://renderer-assets.typeform.com/vendors~form.965f5dedbb854e83c6c8.js	EGtXBKAf[1].htm.2.dr	false		high
http://https://images.typeform.com/images/FYUps4mFKPYK/image/default	EGtXBKAf[1].htm.2.dr	false		high
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~(	imagestore.dat.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://moremi.media/Secure/#com/to/EGtXBKAf.ico	~DF17EE954C7F130427.TMP.1.dr	true	• Avira URL Cloud: phishing	unknown
http://https://public-assets.typeform.com/public/favicon/favicon.ico	EGtXBKAf[1].htm.2.dr	false		high
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c.s	Secure[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://fontawesome.io/license	font-awesome[1].css.2.dr	false		high
http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_account_add_56e73414003cdb676008ff7857343	Secure[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://images.typeform.com/images/DrKa8vFiKNSW/image/default	EGtXBKAf[1].htm.2.dr	false		high
http://https://renderer-assets.typeform.com/form.9cd5d6381506e5950fe0.js	EGtXBKAf[1].htm.2.dr	false		high
http://https://renderer-assets.typeform.com/modern-renderer.36eec26e0148023415c0.js	EGtXBKAf[1].htm.2.dr	false		high
http://https://public-assets.typeform.com/public/favicon/favicon-32x32.png-	imagestore.dat.2.dr	false		high
http://https://github.com/js-cookie/js-cookie	renderer.0f5a683b381b67dbbf89[1].js.2.dr	false		high
http://https://moremi.media/Sypeform.com/to/EGtXBKAf	{51C83D51-5609-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: phishing	unknown
http://https://renderer-assets.typeform.com/vendors~attachment.6e37d3fcdf703c1517e1.js	EGtXBKAf[1].htm.2.dr	false		high
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_grey_5bc252567ef56db648207d9c36a9d004.p	Secure[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.224.100.80	unknown	United States		16509	AMAZON-02US	false
162.247.242.19	unknown	United States		23467	NEWRELIC-AS-1US	false
13.224.94.31	unknown	United States		16509	AMAZON-02US	false
13.224.94.86	unknown	United States		16509	AMAZON-02US	false
13.224.94.88	unknown	United States		16509	AMAZON-02US	false
52.41.92.51	unknown	United States		16509	AMAZON-02US	false
152.199.23.37	unknown	United States		15133	EDGECASTUS	false
167.114.89.121	unknown	Canada		16276	OVHFR	false
104.16.18.94	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339434
Start date:	14.01.2021
Start time:	02:38:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://bgcaustralia.typeform.com/to/EGtXBKAf
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:	10
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

Copyright null 2021

Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.phis.win@3/31@13/9
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://moremi.media/Secure/
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 13.88.21.125, 168.61.161.212, 88.221.62.148, 104.18.27.71, 104.18.26.71, 151.101.2.110, 151.101.66.110, 151.101.130.110, 151.101.194.110, 51.104.139.180, 209.197.3.24, 92.122.213.194, 92.122.213.247, 152.199.19.161, 52.155.217.156 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, cds.s5x3j6q5.hwcdn.net, arc.msn.com.nsatc.net, ie9comview.vo.msecnd.net, displaycatalog.md.mp.microsoft.com.akadns.net, f4.shared.global.fastly.net, aadcdnoriginneu.azureedge.net, skypedataprdcolcus17.cloudapp.net, a1449.dscg2.akamai.net, arc.msn.com, aadcdnoriginneu.ec.azureedge.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, random.typeform.com.cdn.cloudflare.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, skypedataprdcolwus15.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\E5F0NRSV\bgcaustralia.typeform[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):	103826
Entropy (8bit):	5.369161957073601
Encrypted:	false
SSDEEP:	768:TU7U6CfUFC4UFCxUFC/UFCbUFCKUFC7UFCICACICw5+5uBiBWrXOTCCFvssMqHQi:ErXOTCCFvssMqHQ1mRXddhOz1XcEW
MD5:	A7CD975EA3700676CE2740B1182A58AE
SHA1:	211D4115EF6F12D3AEC1A153B8CC272385C39459
SHA-256:	14F965ABBE0226FBE3642264E6F87AAE79D00004D76BBA27C4C0F297F46E1E52
SHA-512:	3E25D25B7805827D681461762C500561BAF5BD75CF1C685D37BF88A33206E3CEB1369AC639B3C8CAB202FB4C87EEABE76DC0B2BB941E678978698053D7C9CF2D
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="EGtXBKAf-visitorId" value="EGtXBKAf-1610588364391-70" ltime="379781584" htime="30861846" /></root><root><item name="EGtXBKAf-visitorId" value="EGtXBKAf-1610588364391-70" ltime="379781584" htime="30861846" /><item name="074c3a45-79fb-43bc-bec4-710ee2d31ed1" value="test_value" ltime="383291584" htime="30861846" /></root><root><item name="EGtXBKAf-visitorId" value="EGtXBKAf-1610588364391-70" ltime="379781584" htime="30861846" /></root><root><item name="EGtXBKAf-visitorId" value="EGtXBKAf-1610588364391-70" ltime="379781584" htime="30861846" /><item name="debug" value="undefined" ltime="383291584" htime="30861846" /></root><root><item name="EGtXBKAf-visitorId" value="EGtXBKAf-1610588364391-70" ltime="379781584" htime="30861846" /><item name="debug" value="undefined" ltime="383441584" htime="30861846" /></root><root><item name="EGtXBKAf-visitorId" value="EGtXBKAf-1610588364391-70" ltime="379781584" htime="30861846" /><item name="debug" value="undefined" ltime=""

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{51C83D4F-5609-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8451831907761556
Encrypted:	false
SSDEEP:	192:rGZ1ZP2w9W8tbifGyYzMAgBxmDZsffy1jX:rC7ewUI8LVico
MD5:	8E2704CF1C31A8F865332E5A73823F0B
SHA1:	E1515C5D2D22558A898AAC0C8AA30D7678E60DA2
SHA-256:	7A928A350A4D03EFD5BF80C8F3943177DC2F61DA0B361D454B43DB0E74C6E9DA
SHA-512:	5A68B227B9322087AC9FC784E9C6D988F55BCF5A2327515E627B2A5B4A59C9C9D6C6126837394164712F7813836B3788FDE4CACF1623FDD09D34D95985420B38
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\{51C83D51-5609-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	49252
Entropy (8bit):	2.0437922929773844
Encrypted:	false
SSDEEP:	192:rsZzQS60kLFjB2gkW9MMYT02Y0HYTRPi6egHEw+6HpVtHEB6m/vJ7txRs20JbtEQ:rs89ZLhwkOMWifw/QovBt10xtNjjFuY
MD5:	5269E80D839597CC381FF9B41EF448E1
SHA1:	B588FA20BFABABE392A2094BFF693E65223ACDB7
SHA-256:	6F52EC4CF48EFA9ED37BFE93BBDBBCD23B94C26AB83746BBC37A777DE7F6F859

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{51C83D51-5609-11EB-90EB-ECF4BBEA1588}.dat	
SHA-512:	7876E2C5189ACD5699C0D6EAE84BA5609F8F9195A745D3432AAF864D3EDDC77A45A836BE4E7F26BAF1516B1337A26DD53096EE50869B74EB5FD8A4C64997AB36
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\{51C83D52-5609-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5644232878091182
Encrypted:	false
SSDEEP:	48:IwmGcprMGwpaRG4pQ1GrapbSYrGQpKaUG7HpRNosTGIpG:r6ZkQD6lBSYFAafTNo4A
MD5:	DA7C7806963BEE62C7628FEF47F9FC0B
SHA1:	415386E8829A86DB87BBBF8CBF88A5941E6D8D14
SHA-256:	849F67B2D5D61E74C172ED37BBDAF7405DB5F969374CC39C1330DDA4593B54D3
SHA-512:	BF7C948986B5F9E0919B8CDD857F8FF46C001E31AC0EC211B41DF5B472923E9AEFB2BFCA4E6569C8EAFD43288FA57BD2AE6707C2E25EB47CBCB2A82E1FE7A786
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	19741
Entropy (8bit):	3.6055381038036196
Encrypted:	false
SSDEEP:	48:YUx0v9PoQ5VqKwspEe6hYJ5eJ5LJ5zJ5YgyyyyyyyyyyyyyzJ5KGJ5/QQQQQZ:mHJE33cP9QQQQQZ
MD5:	F52CB5CFAE03718F72C7FB2C9DCB540D
SHA1:	81909DA8BC8977A99C698CB76C74B6817FC2F0C4
SHA-256:	369618CC921F77103F1E2AA5224FFA67450D16D014A561CAF357C4AEDB6D38AB
SHA-512:	D032E3C98BB6DDCDBCC8D96B1C3A77998D8E2CAA8F96481313C216752DFCDD549A9E77E2EDE8631FB059B6245B541511F28E750CF343C36353C900B0B13684
Malicious:	false
Reputation:	low
Preview:	C.h.t.t.p.s.:././.p.u.b.l.i.c.-.a.s.s.e.t.s...t.y.p.e.f.o.r.m...c.o.m./.p.u.b.l.i.c./.f.a.v.i.c.o.n./.f.a.v.i.c.o.n.-.3.2.x.3.2...p.n.g.-....PNG.....IHDR... ... .s.....gAMA.....a.... cHRM..z &.....u0...`.:....p..Q<....bKGD.....tIME.....-.....IDATH..MhTW...sn.5L..7!F..I...F..UQhT.....R(..jA..`Q*..... IKM..A.I.Q'?..;o...t2If.~..x.{....C...2..P..C.>~..!0L.....I...=\ .W.-."I.K.H,r...V..!.v9Z?.ze..>.Ry.N..Jm..?..*..b..~..*..+O.i.).2}....1.BY.....L.(.aM.....?...f ..._.X...T.Z.f..S.{.#..{...Op.Y.87..X.9...[.,.$..Z|oV{..c.|#_c.. ....!.0..t.gs...X{c..6G.X.9.. ..".e.....u4.",...G9'.NqN.....`..._..p.K[5..%.:0.7...zSh.7Q......./L.2..2.x.Qj.....9 .$-.e88... ..G.YF.G....b.C.[%.u..c...q#.6..5....<...-...`.;..7..0....S.~.2....[...|...:-.`....;..p.O....Z` .....>.4|"|.....P}._...C.U....HX.5t.3..SH...R{U..^BV.=.m.vW.....>..i....oM.g...\}....v.j.n...'Z:..j...TP!U.NM.}..&.=x'3.B...w>..GE..8.....[r.9C/...d;.PH....3.m....[._ .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\2_bc3d32a696895f78c19df6c717586a5d[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1864
Entropy (8bit):	5.222032823730197
Encrypted:	false
SSDEEP:	48:yvswNIBLBpJawmMH44log6gw/MHm7pJroog6gwkMH9Xog6gwdMHdqdyqog7C:ykfXYx+odPcs9B
MD5:	BC3D32A696895F78C19DF6C717586A5D
SHA1:	9191CB156A30A3ED79C44C0A16C95159E8FF689D
SHA-256:	0E88B6FCBB8591EDFD28184FA70A04B6DD3AF8A14367C628EDD7CABA32E58C68
SHA-512:	8D4F38907F3423A86D90575772B292680F7970527D2090FC005F9B096CC81D3F279D59AD76EAFCA30C3D4BBAF2276BBAA753E2A46A149424CF6F1C319DED5A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\2_bc3d32a696895f78c19df6c717586a5d[1].svg	
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6z" fill="url(#A)"/><path d="M394.2 1815.6c746.58 0 1351.8-493.2 1351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 1815.6 394.2 1815.6z" fill="url(#B)"/><path d="M1548.6 1885.2c631.92 0 1144.2-417.45 1144.2-932.4S2180.52 20.4 1548.6 20.4 404.4 437.85 404.4 952.8s512.276 932.4 1144.2 932.4z" fill="url(#C)"/><path d="M265.8 1215.6c690.246 0 1249.8-455.595 1249.8-1017.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUnits="userSpaceOnUse" gradientTransform="translate(1466.4 393.6) rotate(90) scale(1401.6 1720.8)"><stop stop-color="#107c10"/><stop offset="1" stop-color="#c4c4c4" stop-opacity="0"/></radialGradient><r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\EGtXBKAf[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):	122355
Entropy (8bit):	5.3708380351104825
Encrypted:	false
SSDEEP:	1536:qpZaX8ynI1Z4tG81pMH/+eA/7D5GccKppVCJ05vbwIFhnLd71UDWfeiynmn9Tv3i:6zInp7eDFnQyV8kAhvzwqy
MD5:	F6290649EC4ACC55E36BA4B0630F41A1
SHA1:	E1FCADF21DC807CC5AAE0F86F951745C43D2D239
SHA-256:	F867C83E236C6FD172C26C47F36D4238CB19761559C391D7BEFEF74BD107F267
SHA-512:	CC8E6433273F84402E5F83C184F7B706AB38D05CFFC69FCA3A9CA2B0D0987563278C86E9BD37333CED570F2685A18E58373EB027223EE916A22C18A2FC3013E
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html><html lang="en"><head><title>New typeform</title><meta charSet="utf-8"/><meta content="#FFFFFF" name="theme-color"/><meta content="width=device-width, initial-scale=1.0, viewport-fit=cover" name="viewport"/><meta content="Turn data collection into an experience with Typeform. Create beautiful online forms, surveys, quizzes, and so much more. Try it for FREE." name="description"/><meta content="ie=edge" http-equiv="x-ua-compatible"/><meta content="yes" name="apple-mobile-web-app-capable"/><meta content="noindex,nofollow" name="robots"/><meta content="no-referrer-when-downgrade" name="referrer"/><meta content="#000000" name="msapplication-TileColor"/><meta content="https://public-assets.typeform.com/public/favicon/browserconfig.xml" name="msapplication-config"/><link href="https://public-assets.typeform.com/public/favicon/apple-touch-icon.png" rel="apple-touch-icon" sizes="180x180"/><link href="https://public-assets.typeform.com/public/favicon/favicon-32x32.png" rel="icon"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Secure[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	116336
Entropy (8bit):	5.3816220537602755
Encrypted:	false
SSDEEP:	1536:Yhuhw+ExmazA/PWrF7qvEAFiQcpmNtuhPyJRp7xvnXE1Esns8lR:Yt4wyJjZnXE1Esns8H
MD5:	3752C84E2D4118729A264E7629A62E88
SHA1:	22C6C7C155B63E6F566BF554406A5F0780C3F800
SHA-256:	94860511EBE34294BA25E9D70248BA9855B1743CF7CB88796605494C130582D5
SHA-512:	BFCBFC34FD403CD7CBE119C697E1D71AF7F83E83C2BAD190852502C2CEC0669D117AAFB824BB0422667DAEC66D819F7FC40205AFB94C09CB4376572972CAE03
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Secure[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://moremi.media/Secure/
Preview:	<html dir="ltr" lang="en">.. <meta charset="utf-8">.. <link href="https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico" rel="shortcut icon">.. <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css" integrity="sha256-NuCn4IvuZXdBaFKJOAcsU2Q3ZpwbdFisd5dux4jkQ5w=" crossorigin="anonymous">.. <style>... html{font-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,menu,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background-color:transparent}a:active,a:hover{outline:0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:bold}dfn{font-style:italic}h1{font-size:2em;margin:.67em 0}mark{background:#ff0;color:#000}small{font-size:80%}sub,sup{font-size:75%

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\favicon_a_eupayfgghqiai7k9sol6lg2[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 6 icons, 128x128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsQZp:nfgyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\favicon_a_eupayfgghqiai7k9sol6lg2[1].ico	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico
Preview:	.....h(..f...HH.....(..00.....h....6.. .....=.....@.....(....A..(.....(......"P.....""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\renderer.0f5a683b381b67dbbf89[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://renderer-assets.typeform.com/renderer.0f5a683b381b67dbbf89.js
Preview:	window.renderer=function(e){function t(t){for(var n,o,i=t[0],a=t[1],u=0,l=[];u<i.length;u++)o=i[u],Object.prototype.hasOwnProperty.call(r,o)&&r[o]&&l.push(r[o][0]),r[o]=0;for(n in a)Object.prototype.hasOwnProperty.call(a,n)&&(e[n]=a[n]);for(c&&c(t);l.length;)l.shift()()}var n={},r={3:0};function o(t){if(n[t])return n[t].exports;var r=n[t]={i:t,l:!1,exports:{}};return e[t].call(r.exports,r,r.exports,o),r.l=!0,r.exports}o.e=function(e){var t=[],n=r[e];if(0!==n)if(n)t.push(n[2]);else{var i=new Promise((function(t,o){n=r[e]=[t,o]}));t.push(n[2]=i);var a,u=document.createElement("script");u.charset="utf-8",u.timeout=120,o.nc&&u.setAttribute("nonce",o.nc),u.src=function(e){return o.p+""+({0:"blocks-matrix",1:"form",2:"phonenumber",4:"vendors~attachment",5:"vendors~blocks-ranking",6:"vendors~form",7:"vendors~phonenumber"}[e]||e)+"."+{0:"0544beec0e1a4e11a24a",1:"9cd5d6381506e5950fe0",2:"6ea5ec50b9fa21e816ff",4:"6e37d3fcdf703c1517e1",5:"f8aee16223a106724ea1",6:"965f5dedbb854e83c6c8",7:"32d78847

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\analytics.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	356061
Entropy (8bit):	5.3421494353818195
Encrypted:	false
SSDEEP:	3072:X0GSREKFgJ8O0W8U2CtdZsE0nlZSfFp1Jv36yMtkcJsh+qykB:kGcEcfCtdZsE6lk7IuuC
MD5:	C972CB2152B4CA69E1AD84AD369E5D49
SHA1:	2D408DC4AA2394089E145D4619793835A5745AB4
SHA-256:	18FBDEDB7C4B401C5FFA1A76F429FEECEC9928679D485A0CE3F2EA90F709B61E
SHA-512:	3F3294A19D98A64C76929F3F098982B210D83E2FD55487B0B05010D5E073633770C697773682FE053A015CBAD3F316DE2211948F8D5DB2A0974E95BCD09D4FF6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.segment.com/analytics.js/v1/9at6spGDYXelHDdz4r0cP73b3wV1f0ri/analytics.min.js
Preview:	!function(define){"function"==typeof define&&define.amd&&(define=undefined);!function(){function e(t,n,o){function i(r,s){if(!n[r]){if(!t[r]){var u="function"==typeof require&&require;if(!s&&u)return u(r,!0);if(a)return a(r,!0);var l=new Error("Cannot find module '"+r+"'");throw l.code="MODULE_NOT_FOUND",l}var d=n[r]={exports:{}};t[r][0].call(d.exports,function(e){return i(t[r][1][e]||e)},d,d.exports,e,t,n,o)}return n[r].exports}for(var a="function"==typeof require&&require,r=0;r<o.length;r++)i(o[r]);return i}return e}({1:[function(e,t,n){"use strict";var o=e("@segment/analytics.js-core"),i=e("@ndhoule/each");t.exports=function(e){i(function(e){o.use(e)},e);return o}},{"@ndhoule/each":32,"@segment/analytics.js-core":76}],2:[function(e,t,n){(function(n){"use strict";var o=e("@segment/send-json");t.exports=function(){for(var e=!1,t=!1,i=/.*\Analytics\.js\/v1\/([^/]*)(\/platform)?\/analytics.*/,a=n.document.getElementsByTagName("script"),r=0;r<a.length;r++){var s=a[r].src,u=i.exec(s);i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\font-awesome[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	troff or preprocessor input, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	37414
Entropy (8bit):	4.82325822639402
Encrypted:	false
SSDEEP:	768:mmMtI+A4CSIDqvnI+YTBrFPvVrJjhiRAiiEL:mXtI+A4GDUI+Y9rpVljhiIEL
MD5:	C495654869785BC3DF60216616814AD1
SHA1:	0140952C64E3F2B74EF64E050F2FE86EAB6624C8
SHA-256:	36E0A7E08BEE65774168528938072C536437669C1B7458AC77976EC788E4439C
SHA-512:	E40F27C1D30E5AB4B3DB47C3B2373381489D50147C9623D853E5B299364FD65998F46E8E73B1E566FD79E97AA7B20354CD3C8C79F15372C147FED9C913FFB10
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css
Preview:	/*!. * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */./* FONT PATH. * -------------------------- */.@font-face {. font-family: 'FontAwesome';. src: url('../fonts/fontawesome-webfont.eot?v=4.7.0');. src: url('../fonts/fontawesome-webfont.eot?#iefix&v=4.7.0') format('embedded-opentype'), url('../fonts/fontawesome-webfont.woff2?v=4.7.0') format('woff2'), url('../fonts/fontawesome-webfont.woff?v=4.7.0') format('woff'), url('../fonts/fontawesome-webfont.ttf?v=4.7.0') format('truetype'), url('../fonts/fontawesome-webfont.svg?v=4.7.0#fontawesomeregular') format('svg');. font-weight: normal;. font-style: normal;.}..fa {. display: inline-block;. font: normal normal normal 14px/1 FontAwesome;. font-size: inherit;. text-rendering: auto;. -webkit-font-smoothing: antialiased;. -moz-osx-font-smoothing: grayscale;.}./* makes the font 33% larger relative to the icon container */..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\form.9cd5d6381506e5950fe0[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):	227059
Entropy (8bit):	5.280936780615679
Encrypted:	false
SSDEEP:	3072:5hjrDWVbCG3oaMZ7wLNM5NTM20ZPL4BrWN0QzFI+VDvoDa9f:6Vb0aMsQlMBPLUr58dDvsm
MD5:	DD7F1393ACBF039DA8D9970914488D42
SHA1:	6471C4824923D895CCE1D956F1D93CC6C57AB9EF
SHA-256:	3DF9AAE60EBE3300471A343673C3771D554934DDA473CE495CD0539AEF8872A0
SHA-512:	C3E97929DABD62E75D54C47E5D6E59630407FF1FEA5BE94D4B2C8BC131541FAD1008D99294FE39887C468A951B951C0A4C2BF32DEA33901BEF1296CB336061F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\form.9cd5d6381506e5950fe0[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://renderer-assets.typeform.com/form.9cd5d6381506e5950fe0.js
Preview:	(window.webpackJsonp_name_=window.webpackJsonp_name_||[]).push([[1],{236:function(e,t,n){"use strict";n.d(t,"a",(function(){return o})),n.d(t,"b",(function(){return a})); var r=n(10),o=function(){return{type:r.t,payload:{}}},a=function(){return{type:r.F,payload:{}}}},237:function(e,t,n){"use strict";n.d(t,"b",(function(){return o})),n.d(t,"a",(function(){return a}));var r=n(10);function o(e){return{type:r.A,payload:e}}function a(e){return{type:r.z,payload:e}}},238:function(e,t,n){"use strict";n.d(t,"b",(function(){return je})),n.d(t,"a",(function(){return Ee}));var r=n(80),o=n.n(r),a=(n(158),n(117)),c=n.n(a),i=n(3),u=n(26),s=n(75),l=n(6),p=n(505);n(442);var d=n(150),f=(n(24),n(506),n(507),n(6 08),n(20),n(13)),b=n.n(f),m=n(615),h=n.n(m),v=n(609),g=n.n(v),y=n(2),O=n.n(y),j=n(225),w=(n(22),n(29),n(472),n(84),n(208)),k=n.n(w),x=function(e){var t=e.split("-"),n=b() (t,3),r=n[0],o=n[1],a=n[2];if(!r||!o||!a)return!1;r=r.padStart(4,"0"),o=o.padStart(2,"0"),a=a.padStart(2,"0");var c=new Date(""".co

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\53_8b36337037cff88c3df203bb73d58e41[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 342 x 72, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	5139
Entropy (8bit):	7.865234009830226
Encrypted:	false
SSDEEP:	96:oX2DsRVNYc82nTGTirCPqKO1gDPFjDiwK3aM5yO/bUlVV6JKo5N9jIMw7RLW1ZHb:ofRgc82nTprQsgDNDP7QgVVoH9+kMK9
MD5:	8B36337037CFF88C3DF203BB73D58E41
SHA1:	1ADA36FA207B8B96B2A5F55078BFE2A97ACEAD0E
SHA-256:	E4E1E65871749D18AEA150643C07E0AAB2057DA057C6C57EC1C3C43580E1C898
SHA-512:	97D8CC97C4577631D8D58C0D9276EE55E4B80128080220F77E01E45385C20FE55D208122A8DFA5DADCB87543B1BC291B98DBBA44E8A2BA90D17C638C15D487
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/applogos/53_8b36337037cff88c3df203bb73d58e41.png
Preview:	.PNG.....IHDR...V...H.....tEXtSoftware.Adobe ImageReadyq.e<...%iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop 21.0 (Macintosh)" xmpMM:InstanceID="xmp.iid:DB120779422011EA9888910153D3A5E6" xmpMM:DocumentID="xmp.did:DB12077A422011EA9888910153D3A5E6"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:DB120777422011EA9888910153D3A5E6" stRef:documentID="xmp.did:DB120778422011EA9888910153D3A5E6"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>P.WI....IDATx..]]l.....(.5. K0P..0...E.qT..J X)F.(5X....J.}(m.R5.Q...RUEUPU~.....qp@.b.....L...k.m"0....."c.3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\aa6e0ec721[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.340020120659463
Encrypted:	false
SSDEEP:	3:U3KTDW3MiqVkMWVrfUh:H6NukMWVr8h
MD5:	06DD80AEB628C60DC680BC7A4BEE6651
SHA1:	8C86EB7DDFF5E1E5D527BD7A41C9D3F6767E23E0
SHA-256:	5E864C2E3F674C60970513411EAEEEAFD2D615D842E65EC01D09CCFCB4A7B38D
SHA-512:	C6EE8252743A760AD7BEE017FF7A804B6E34236764BC5630289D5E4C7C15E38CB971F161821586F0235882FD581630F1531FD6396761BF1284581CD8C2CAC4C6
Malicious:	false
Reputation:	low
Preview:	NREUM.setToken({'stn':0,'err':1,'ins':1,'cap':0,'spa':1})

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	513
Entropy (8bit):	4.720499940334011
Encrypted:	false
SSDEEP:	12:t4BdU/uRqv6DLfBHKFWJCDLfBSU1pRXIFl+MJ4bADc:t4TU/uRff0EcfIU1XXU+t2c
MD5:	A9CC2824EF3517B6C4160DCF8FF7D410
SHA1:	8DB9AEBAD84CA6E4225BFDD2458FF3821CC4F064
SHA-256:	34F9DB946E89F031A80DFCA7B16B2B686469C9886441261AE70A44DA1DFA2D58
SHA-512:	AA3DDAB0A1CFF9533F9A668ABA4FB5E3D75ED9F8AFF8A1CAA4C29F9126D85FF4529E82712C0119D2E81035D1CE1CC491FF9473384D211317D4D00E0E234AD9F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410[1].svg	
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="24" height="24" viewBox="0 0 24 24"><title>assets</title><path d="M18,11.578v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944.594.594L7.617,11.578Z" fill="#404040"/><path d="M10.944,7.056l.594.594L7.617,11.578H18v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944m0-.141-.071.07L5.929,11.929,5.858,12l.071.071,4.944,4.944.071.07.071-.07.594-.595.071-.07-.071-.071L7.858,12.522H18.1V11.478H7.858l3.751-3.757.071-.071-.071-.07-.594-.595-.071-.07Z" fill="#404040"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\ellipsis_635a63d500a92a0b8497cdc58d0f66b1[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	900
Entropy (8bit):	3.8081778439799248
Encrypted:	false
SSDEEP:	24:t4CvnAVRHf1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUV0Uv6f1QqCWbVHTVeUV0UFl:fn+1QqC4GuiHFXS1QqCWRHQ3V1QqCWRV
MD5:	635A63D500A92A0B8497CDC58D0F66B1
SHA1:	A32EBA4B4D139E8DA52C5801A13C1EE222B2B882
SHA-256:	61D7CCC5D2C41BF86BE6CEFB0063405067849BA64E9F219F60596EF09A54A942
SHA-512:	EFFE15E105FC5FA853E76917B533AAE6C75EBA9A256049FB5EAB88BBF319D63A4CE4AE3743A09D6A5F474B01649D6EDC5C8BCCC61B8CA9EA9E5C39E7AE724C16
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_635a63d500a92a0b8497cdc58d0f66b1.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path d="M1.143,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,.7,9.054a1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893A1.164,1.164,0,0,1,.7,6.946a1.107,1.107,0,0,1,.446-.089M8,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1-.607-.607A1.107,1.107,0,0,1,8,6.857m6.857,0a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,14.857,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	915
Entropy (8bit):	3.8525277758130154
Encrypted:	false
SSDEEP:	24:t4CvnAVRfFArf1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUVx:fn1r1QqC4GuiHFXS1QqCWRHQ3V1QqCWz
MD5:	2B5D393DB04A5E6E1F739CB266E65B4C
SHA1:	6A435DF5CAC3D58CCAD655FE022CCF3DD4B9B721
SHA-256:	16C3F6531D0FA5B4D16E82ABF066233B2A9F284C068C663699313C09F5E8D6E6
SHA-512:	3A692635EE8EBD7B15930E78D9E7E808E48C7ED3ED79003B8CA6F9290FA0E2B0FA3573409001489C00FB41D5710E75D17C3C4D65D26F9665849FB7406562A406
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path fill="#777777" d="M1.143,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,.7,9.054a1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893A1.164,1.164,0,0,1,.7,6.946a1.107,1.107,0,0,1,.446-.089M8,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607A1.107,1.107,0,0,1,8,6.857m6.857,0a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607A1.107,1.107,0,0,1,14.857,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\favicon-32x32[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	1069
Entropy (8bit):	7.54915864947209
Encrypted:	false
SSDEEP:	24:pym4kMz0v9Pb0B8EkKHUNnVqKy19szgpzGEMAp02Efl9:E0v9PoQ5VqKwspEeT
MD5:	4A35A27936C43081F0865E2E603DF15D
SHA1:	A6D584D829C87EFF74C08F770CD2EF78EE75742E
SHA-256:	DCAE3697C63FCB6AE03D2FD99FB96AF8B14848B71A259ED2E05DBCF5CEDEA5B2
SHA-512:	5DB18A7D2A60BD729F6F12E8A9B05F7A15E90C68CF3415993E8A5B1DB2B5BBA0D4B34B3F2A989E47C7495B9CF202703F0E50694E8865B0784A88EC1A40AF878
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://public-assets.typeform.com/public/favicon/favicon-32x32.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\favicon-32x32[1].png	
Preview:	.PNG.....IHDR... ... .s.....gAMA.....a.... cHRM..z&.....u0...`..:....p..Q<....bKGD.....tIME.....-.....IDATH..MhTW...sn.5L..7!F..I...F..UQhT.....R(..jA..`Q*..... IKM..A.I.Q'?..;o...t2If.~..x.{....C...2..P..C.>~..!0L.....I...=\.W.-."I.K.H,r...V..!.v9Z?.ze..>.Ry.N..Jm..?..*..b..~..*..+O.i.).2}....1.BY.....L.(.aM.....?...f ..._.X...T.Z.f..S.{.#..{...Op.Y.87 ..X.9...[.,.$..Z\|oV{..c.\|#_c.. ....!.0..t.gs...X{c..6G.X.9....".e.....u4.",...G9'.NqN.....`..._..p.K[5..%.:0.7...zSh.7Q......./L.2..2.x.Qj.....9 .$-.e88... ..G.YF.G....b.C.[%.u..c... q#.6..5....<...-...`.;..7..0....S.~.2....[...|...:-.`....;..p.O....Z` .....>.4|"|.....P}._...C.U....HX.5t.3..SH...R{U..^BV.=.m.vW.....>..i....oM.g...\}....v.j.n...'Z:..j...TP!U.NM.}..&.=x'3.B...w>. .GE..8.....[r.9C/...d;.PH....3.m....[._ .....%tEXtdate:create.2021-01-04T13:10:14+01:00yu.}...%tEXtdate:modify.2021-01-04T13:10:14+01:00.(g....WzTXtRaw profile type iptc..x.....qV((.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38 .119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1.392, 1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47. 081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0, 0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.61 1,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.9 52,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\picker_account_aad_9de70d1c5191d1852a0d5aac28b44a6c[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	756
Entropy (8bit):	4.879179443781471
Encrypted:	false
SSDEEP:	12:t4pb8WsQKvkBWSfYcW3ffBfYfomQO1a7aajR2F1hgWSnuCNSganii7v/NPujARqj:t4pb8WvKMTfY3ffBfYfomQO1eXjR2oug
MD5:	9DE70D1C5191D1852A0D5AAC28B44A6C
SHA1:	F4F64F5CBDBE6D1115C10A7F9CCB8828E6B67CAE
SHA-256:	5D3357BD875B7335ACE42E8EE3A64578E4253BED1A4E279109DE403EEDAE3A69
SHA-512:	CAC13FC2FE30E10772008F2AFF70FCA031EA9918E1F8C5C8B91CB9E79463383183406EFAADF89360DE3A08573FCDF2716C14DA6411E24B7E260B96AF84F0076
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_account_aad_9de70d1c5191d1852a0d5aac28b44a6c.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="48" height="48" viewBox="0 0 48 48"><title>assets</title><circle cx="24" cy="24" r="24" fill="#e6e6e6"/><path d=" M34,35V14a2.938,2.938,0,0,0-3-3H27V8l2-1L27.948,5.638,24,8,20.07,5.648,19,7l2,1v3H17a2.938,2.938,0,0,0-3,3V35a2.938,2.938,0,0,0,3,3H31A2.938,2.938,0,0 ,0,34,35Zm-3,1H17a.979.979,0,0,1-1-1V14a.979.979,0,0,1,1-1h6V10h2v3h6a.979.979,0,0,1,1,1V35A.979.979,0,0,1,31,36Z" fill="#404040"/><path d="M26.766,25 .42a4.432,4.432,0,1,0-5.533,0A6.237,6.237,0,0,0,17.765,31h1.653a4.582,4.582,0,1,1,9.165,0h1.653A6.237,6.237,0,0,0,26.766,25.42Zm-5.546-3.435A2.779,2.779,0,1,1,2 4,24.765,2.783,2.783,0,0,1,21.221,21.985Z" fill="#404040"/><rect x="21" y="14" width="6" height="2" rx="1" ry="1" fill="#404040"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\picker_account_add_56e73414003cdb676008ff7857343074[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	222
Entropy (8bit):	5.004415423297573
Encrypted:	false
SSDEEP:	3:tIsqDmJS4RKb5zMc7XpCN+bJMacvRxyJAgR/QvfqhcDQKG2TcVER+HLZqWTboZUq:tI9mc4slztdbC/yXADQKDTcVEqLwDZsc
MD5:	56E73414003CDB676008FF7857343074
SHA1:	9ED7A58CD0E81E9689AC8C6D548A47D0185E0FDC
SHA-256:	749F85621D92A5B31B2A377A8C385A36D48A83327DAD9A8A8DA93CD831B8C9A2
SHA-512:	FAD0071AC2DFA23989BFBC7D3850415F3C340A74A54D3D8D797AFCCD6A301513BBC769DF4E5148605BE1E23A8750973EB80726F3CC959A2A457B0EC09AE14F 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_account_add_56e73414003cdb676008ff7857343074.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\picker_account_add_56e73414003cdb676008ff7857343074[1].svg	
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="48" height="48" viewBox="0 0 48 48"><title>assets</title><circle cx="24" cy="24" r="24" fill="#e6e6e6"/><path d="M25,23H36v2H25V36H23V25H12V23H23V12h2Z" fill="#404040"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\picker_more_7568a43cf440757c55d2e7f51557ae1f[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	899
Entropy (8bit):	3.8260330857236338
Encrypted:	false
SSDEEP:	24:t4CvnAVROLgCWbVHTVSRUyL3Fe09gCWbVHTVeUVh10UsSgCWbVHTVeUVh10Usb7:fncCWRH0JL3FECWRHQA10rCWRHQA10F
MD5:	7568A43CF440757C55D2E7F51557AE1F
SHA1:	55C22CA98B5CDCED134F6E24205C288845312A2D
SHA-256:	B7FCD37EAAFE3F08647ED072D5289EADFFF6C660A26CDEF31532B3FCFB4A0BB2
SHA-512:	F01DA2804594C3C78C0694FD6CC49B667663DA95AE7367EE3F0F5112B9957A3220389AAE4A5B750BCB3BC4F1092EA614266A4BFFD7E0FE16232E1CB57606E90
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_more_7568a43cf440757c55d2e7f51557ae1f.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path d="M9.143,1.143a1.107,1.107,0,0,1-.089.446,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.107,1.107,0,0,1-.089-.446A1.107,1.107,0,0,1,6.946.7,1.164,1.164,0,0,1,7.554.089a1.161,1.161,0,0,1,.893,0A1.164,1.164,0,0,1,9.054.7a1.107,1.107,0,0,1,.089.446M9.143,8a1.107,1.107,0,0,1-.089.446,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607,1.161,1.161,0,0,1,.893,0A1.164,1.164,0,0,1,9.143,8m0,6.857a1.107,1.107,0,0,1-.089.446,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607,1.161,1.161,0,0,1,.893,0,1.164,1.164,0,0,1,.607.607A1.107,1.107,0,0,1,9.143,14.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\aa6e0ec721[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	24
Entropy (8bit):	2.459147917027245
Encrypted:	false
SSDEEP:	3:CUXJ/lH:Dl
MD5:	BC32ED98D624ACB4008F986349A20D26
SHA1:	2D3DF8C11D2168CE2C27E0937421D11D85016361
SHA-256:	0C9CF152A0AD00D4F102C93C613C104914BE5517AC8F8E0831727F8BFBE8B300
SHA-512:	71ACC6DA78D5D5BF0EEA30E2EE0AC5C992B00EFEC959077DFE0AB769F1DBBD9AF12D5C5C155046283D5416BEB606A9EF323FB410E903768B1569B69F37075B4E
Malicious:	false
Reputation:	low
Preview:	GIF89a.....,.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\default[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, baseline, precision 8, 767x239, frames 3
Category:	downloaded
Size (bytes):	13390
Entropy (8bit):	7.76618612493712
Encrypted:	false
SSDEEP:	384:S2RDbWcDD0FcCPR7+LZyv5foCDPzPwRxWcMOOOFvq:bRDycQtRiLkv5ZPzwmVOOOM
MD5:	C1E8EE476900A97C7CB87D18752AF4D7
SHA1:	DA711E2930AA4A150A78ED0F5BB6B31FC7870CCD
SHA-256:	038DCAEECFF5F54E5044D7BF1C101CAA00A260707111AE9959644FCC83BC04BA
SHA-512:	63BFB2A8FE474536EE3FA22ECE3D3CF35617C3C1DAC34AB8979450CDF26A612B13281274D4E1E7D75C8468447F1EA5D13B1BB4506769836EC372CDD8CAB0F27
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://images.typeform.com/images/DrKa8vFiKNSW/image/default
Preview:	.....C.....%...#... , #&')*)..-0-(0%()(...C.....(...(((((((

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\vendors~form.965f5dedbb854e83c6c8[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	418096
Entropy (8bit):	5.702124589125958
Encrypted:	false
SSDEEP:	3072:hO203o4PRjCe7bmD2NF1q2ZG8njVKG85sLGU115ZZQjOurJgR8rrjoP7Gwc4/:hUCkbm6r1q23nkGEsLGgt0a5PKwB
MD5:	6F33B62669DF8B6E094E941BB2F1BB39
SHA1:	D2A46B58E82E30176BDAF55CD018FC89AB9F0C23
SHA-256:	645A6486495927D9FC72EDF35C46B50C990F3DCED2101C79F753F6FA8EC11E16
SHA-512:	D0BDB5C7E927C49908667D60B967D75A0D3D7E05FE09A1F24ED13C2F7E411B6D9B57E140CDD7FE742F3ED7A6364EE6AEB8FC1DB1116364F3B6309A4DE30FC4 82
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://renderer-assets.typeform.com/vendors~form.965f5dedbb854e83c6c8.js
Preview:	(window.webpackJsonp_name_=window.webpackJsonp_name_||[]).push([[6],Array(429).concat([function(e,t,n){"use strict";n.d(t,"a",(function(){return R})),n.d(t,"b", (function(){return v})),n.d(t,"c",(function(){return A})),n.d(t,"d",(function(){return q})),n.d(t,"e",(function(){return l})),n.d(t,"f",(function(){return H})),n.d(t,"g",(function(){return K })),n.d(t,"h",(function(){return P})),n.d(t,"i",(function(){return D})),n.d(t,"j",(function(){return X})),n.d(t,"k",(function(){return re})),n.d(t,"l",(function(){return ae})),n.d(t,"m",(fun ction(){return ne})),n.d(t,"n",(function(){return ce})),n.d(t,"o",(function(){return M})),n.d(t,"p",(function(){return j})),n.d(t,"q",(function(){return L})),n.d(t,"r",(function(){return F})),n.d(t,"s",(function(){return N})),n.d(t,"t",(function(){return le})),n.d(t,"u",(function(){return ee})),n.d(t,"v",(function(){return Z})),n.d(t,"w",(function(){return J})),n.d(t,"x",(funct ion(){return z})),n.d(t,"y",(function(){return oe})),n.d(t,"z",(function(){retur

C:\Users\user\AppData\Local\Temp\~DF17EE954C7F130427.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	53303
Entropy (8bit):	0.949125365268935
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+yU+Xkrfp4iBTPvrevSvkFJ0:9Pv
MD5:	3B5F6BFFC1376332490B3F34AA79DAAA
SHA1:	785A0EC0B18B92ECC4232A3686ABB4B0243F3386
SHA-256:	BAE7DD9A622B823DAA7D1CD80A575FE3ABEB36D9268AE778F15BF290534058FE
SHA-512:	CC8D9861B69EABDE4440B7BCC545D95A1B306B7ED3117561E5592D9094DB0315545D202C5684400CF8CE3A37DF4BC56271C166D604E1292C9532C61E2ECF22
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF34EA67A63D1A1AB6.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47406422150652466
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lom9loW9lWwtjTOxsQ:kBqoIBHwMyQ
MD5:	5EA6708FD076F418099C92ADD402FE3C
SHA1:	657E2854024573CAF4AEB316D8C04BE8AC82A097
SHA-256:	43AB34B5269DC4ABD735622DC412D9F48D02CDB21BE06851E74A8ECC3E21679C
SHA-512:	18C7317125C75E355A33CE0382A9F7A4D765491785CFBBA672ECDE64969EB8E958AFDA6781D102633712C920C81D5DFEC909BAF94E766F5E02389ED8B60C065
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFAC3E7EDAADEA822E.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.28781552615349526

C:\Users\user\AppData\Local\Temp\~DFAC3E7EDAADEA822E.TMP	
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	72E034D903CD43830FC7B657A1CE9D29
SHA1:	2C4F32C57852B89A1580547AF222E7EFD473258D
SHA-256:	3EBD601457CA6CE922131E43B26EDC44548A2621CB59421DE0961CAFEF8B1743
SHA-512:	921BF95C49B3C72ED5014158E964EA8D956131633EC6FDC3F454A301ED501DE4DB6770ACE4516073778916F42B91B2661D49EA18889B637D29255AE3A7429EA5
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 02:39:23.137080908 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.137151003 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.137217045 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.138312101 CET	443	49736	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.138489962 CET	49736	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.138860941 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.139027119 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.158595085 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.159002066 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.159178972 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.159539938 CET	49736	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.159887075 CET	49736	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.204119921 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.204339981 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.204351902 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.204483986 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.204571962 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.204638004 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.204715014 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.204788923 CET	443	49736	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.204802036 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.204965115 CET	443	49736	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.205086946 CET	443	49736	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.205104113 CET	49736	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.205187082 CET	49736	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.205424070 CET	443	49736	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.205435991 CET	443	49736	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.205559969 CET	49736	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.206059933 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.206229925 CET	49736	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.206274033 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.206295967 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.206310034 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.206321955 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.206392050 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.206449032 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.207535982 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.207552910 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.207638025 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.208787918 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.208803892 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.208914995 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.210084915 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.210103989 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.210238934 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.211335897 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.211355925 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.211508036 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.212533951 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.212605000 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.212678909 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.212707996 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.213877916 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.213895082 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.213979006 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.215143919 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.215161085 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.215378046 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.216392994 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.216413975 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.216551065 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.217576981 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.217598915 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.217629910 CET	49737	443	192.168.2.4	13.224.94.31

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 02:39:23.217649937 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.218904018 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.218947887 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.218997955 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.219033957 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.220101118 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.220123053 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.220172882 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.220199108 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.249540091 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.249560118 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.249614000 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.249675989 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.250102997 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.250119925 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.250225067 CET	49737	443	192.168.2.4	13.224.94.31
Jan 14, 2021 02:39:23.251265049 CET	443	49736	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.251409054 CET	443	49737	13.224.94.31	192.168.2.4
Jan 14, 2021 02:39:23.251425028 CET	443	49737	13.224.94.31	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 02:39:17.133217096 CET	49910	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:17.181345940 CET	53	49910	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:18.030870914 CET	55854	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:18.079042912 CET	53	55854	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:19.201229095 CET	64549	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:19.258327961 CET	53	64549	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:20.224550962 CET	63153	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:20.280879974 CET	53	63153	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:21.043390989 CET	52991	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:21.101310015 CET	53	52991	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:21.311413050 CET	53700	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:21.359529018 CET	53	53700	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:22.020625114 CET	51726	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:22.077024937 CET	53	51726	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:22.115125895 CET	56794	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:22.163149118 CET	53	56794	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:22.983819008 CET	56534	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:23.042797089 CET	53	56534	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:23.051506042 CET	56627	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:23.102094889 CET	53	56627	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:23.855547905 CET	56621	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:23.919718981 CET	53	56621	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:23.985531092 CET	63116	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:24.042987108 CET	53	63116	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:24.162710905 CET	64078	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:24.227211952 CET	53	64078	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:25.130794048 CET	64801	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:25.153733015 CET	61721	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:25.178982019 CET	53	64801	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:25.214807987 CET	53	61721	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:25.585567951 CET	51255	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:25.646904945 CET	53	51255	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:26.723946095 CET	61522	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:26.774852037 CET	53	61522	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:32.898633003 CET	52337	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:32.946439981 CET	53	52337	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:33.829463959 CET	55046	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:33.881573915 CET	53	55046	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:34.815619946 CET	49612	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:34.863639116 CET	53	49612	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:35.600919008 CET	49285	53	192.168.2.4	8.8.8.8

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 02:39:35.651721001 CET	53	49285	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:36.665777922 CET	50601	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:36.717535019 CET	53	50601	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:38.737782001 CET	60875	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:38.801287889 CET	53	60875	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:41.061311007 CET	56448	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:41.356723070 CET	53	56448	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:41.498042107 CET	59172	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:41.548759937 CET	53	59172	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:41.956561089 CET	62420	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:42.004729033 CET	53	62420	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:42.115149975 CET	60579	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:42.143017054 CET	50183	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:42.172002077 CET	53	60579	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:42.191591978 CET	53	50183	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:47.344713926 CET	61531	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:47.405437946 CET	53	61531	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:51.009572983 CET	49228	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:51.070924044 CET	53	49228	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:51.646563053 CET	59794	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:51.702948093 CET	53	59794	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:52.016021967 CET	49228	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:52.066879988 CET	53	49228	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:52.655925989 CET	59794	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:52.712555885 CET	53	59794	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:53.030927896 CET	49228	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:53.090414047 CET	53	49228	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:53.672375917 CET	59794	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:53.720480919 CET	53	59794	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:55.004163980 CET	55916	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:55.048732042 CET	49228	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:55.066131115 CET	53	55916	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:55.107831001 CET	53	49228	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:55.539882898 CET	52752	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:55.602271080 CET	53	52752	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:55.687402010 CET	59794	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:55.743684053 CET	53	59794	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:56.145811081 CET	60542	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:56.205782890 CET	53	60542	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:56.575798035 CET	60689	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:56.668579102 CET	53	60689	8.8.8.8	192.168.2.4
Jan 14, 2021 02:39:57.062612057 CET	64206	53	192.168.2.4	8.8.8.8
Jan 14, 2021 02:39:57.110728025 CET	53	64206	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2021 02:39:22.020625114 CET	192.168.2.4	8.8.8.8	0x7872	Standard query (0)	bgcaustralia.typeform.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:22.983819008 CET	192.168.2.4	8.8.8.8	0xa443	Standard query (0)	renderer-assets.typeform.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:23.855547905 CET	192.168.2.4	8.8.8.8	0xe522	Standard query (0)	public-assets.typeform.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:23.985531092 CET	192.168.2.4	8.8.8.8	0x1513	Standard query (0)	js-agent.newrelic.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:24.162710905 CET	192.168.2.4	8.8.8.8	0xf379	Standard query (0)	images.typeform.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:25.130794048 CET	192.168.2.4	8.8.8.8	0x43df	Standard query (0)	bam.nr-data.net	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:25.153733015 CET	192.168.2.4	8.8.8.8	0xcd53	Standard query (0)	cdn.segment.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:25.585567951 CET	192.168.2.4	8.8.8.8	0x51ef	Standard query (0)	api.segment.io	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:38.737782001 CET	192.168.2.4	8.8.8.8	0x33c9	Standard query (0)	public-assets.typeform.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2021 02:39:41.061311007 CET	192.168.2.4	8.8.8.8	0xa59d	Standard query (0)	moremi.media	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:41.956561089 CET	192.168.2.4	8.8.8.8	0x31b	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:42.115149975 CET	192.168.2.4	8.8.8.8	0xc5d	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:42.143017054 CET	192.168.2.4	8.8.8.8	0xa12e	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2021 02:39:22.077024937 CET	8.8.8.8	192.168.2.4	0x7872	No error (0)	bgcaustralia.typeform.com	random.typeform.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:39:23.042797089 CET	8.8.8.8	192.168.2.4	0xa443	No error (0)	renderer-assets.typeform.com	d2citsn5wf4j9j.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:39:23.042797089 CET	8.8.8.8	192.168.2.4	0xa443	No error (0)	d2citsn5wf4j9j.cloudfront.net		13.224.94.31	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:23.042797089 CET	8.8.8.8	192.168.2.4	0xa443	No error (0)	d2citsn5wf4j9j.cloudfront.net		13.224.94.118	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:23.042797089 CET	8.8.8.8	192.168.2.4	0xa443	No error (0)	d2citsn5wf4j9j.cloudfront.net		13.224.94.58	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:23.042797089 CET	8.8.8.8	192.168.2.4	0xa443	No error (0)	d2citsn5wf4j9j.cloudfront.net		13.224.94.129	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:23.919718981 CET	8.8.8.8	192.168.2.4	0xe522	No error (0)	public-assets.typeform.com	d2p6vz8nayi9a3.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:39:23.919718981 CET	8.8.8.8	192.168.2.4	0xe522	No error (0)	d2p6vz8nayi9a3.cloudfront.net		13.224.94.86	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:23.919718981 CET	8.8.8.8	192.168.2.4	0xe522	No error (0)	d2p6vz8nayi9a3.cloudfront.net		13.224.94.107	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:23.919718981 CET	8.8.8.8	192.168.2.4	0xe522	No error (0)	d2p6vz8nayi9a3.cloudfront.net		13.224.94.17	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:23.919718981 CET	8.8.8.8	192.168.2.4	0xe522	No error (0)	d2p6vz8nayi9a3.cloudfront.net		13.224.94.20	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:24.042987108 CET	8.8.8.8	192.168.2.4	0x1513	No error (0)	js-agent.newrelic.com	f4.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:39:24.227211952 CET	8.8.8.8	192.168.2.4	0xf379	No error (0)	images.typeform.com	d2nvsmtq2poimt.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:39:24.227211952 CET	8.8.8.8	192.168.2.4	0xf379	No error (0)	d2nvsmtq2poimt.cloudfront.net		13.224.94.88	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:24.227211952 CET	8.8.8.8	192.168.2.4	0xf379	No error (0)	d2nvsmtq2poimt.cloudfront.net		13.224.94.92	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:24.227211952 CET	8.8.8.8	192.168.2.4	0xf379	No error (0)	d2nvsmtq2poimt.cloudfront.net		13.224.94.25	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:24.227211952 CET	8.8.8.8	192.168.2.4	0xf379	No error (0)	d2nvsmtq2poimt.cloudfront.net		13.224.94.83	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:25.178982019 CET	8.8.8.8	192.168.2.4	0x43df	No error (0)	bam.nr-data.net		162.247.242.19	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:25.178982019 CET	8.8.8.8	192.168.2.4	0x43df	No error (0)	bam.nr-data.net		162.247.242.18	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:25.178982019 CET	8.8.8.8	192.168.2.4	0x43df	No error (0)	bam.nr-data.net		162.247.242.20	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:25.178982019 CET	8.8.8.8	192.168.2.4	0x43df	No error (0)	bam.nr-data.net		162.247.242.21	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:25.214807987 CET	8.8.8.8	192.168.2.4	0xcd53	No error (0)	cdn.segment.com	d296je7bbdd650.cloudfront.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2021 02:39:25.214807987 CET	8.8.8.8	192.168.2.4	0xcd53	No error (0)	d296je7bbdd650.cloudfront.net		13.224.100.80	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:25.646904945 CET	8.8.8.8	192.168.2.4	0x51ef	No error (0)	api.segment.io		52.41.92.51	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:25.646904945 CET	8.8.8.8	192.168.2.4	0x51ef	No error (0)	api.segment.io		54.70.113.89	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:25.646904945 CET	8.8.8.8	192.168.2.4	0x51ef	No error (0)	api.segment.io		35.164.248.150	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:25.646904945 CET	8.8.8.8	192.168.2.4	0x51ef	No error (0)	api.segment.io		35.164.88.121	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:25.646904945 CET	8.8.8.8	192.168.2.4	0x51ef	No error (0)	api.segment.io		52.89.79.226	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:25.646904945 CET	8.8.8.8	192.168.2.4	0x51ef	No error (0)	api.segment.io		52.88.208.102	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:25.646904945 CET	8.8.8.8	192.168.2.4	0x51ef	No error (0)	api.segment.io		35.164.219.175	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:25.646904945 CET	8.8.8.8	192.168.2.4	0x51ef	No error (0)	api.segment.io		54.213.130.70	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:38.801287889 CET	8.8.8.8	192.168.2.4	0x33c9	No error (0)	public-assets.typeform.com	d2p6vz8nayi9a3.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:39:38.801287889 CET	8.8.8.8	192.168.2.4	0x33c9	No error (0)	d2p6vz8nayi9a3.cloudfront.net		13.224.94.107	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:38.801287889 CET	8.8.8.8	192.168.2.4	0x33c9	No error (0)	d2p6vz8nayi9a3.cloudfront.net		13.224.94.17	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:38.801287889 CET	8.8.8.8	192.168.2.4	0x33c9	No error (0)	d2p6vz8nayi9a3.cloudfront.net		13.224.94.86	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:38.801287889 CET	8.8.8.8	192.168.2.4	0x33c9	No error (0)	d2p6vz8nayi9a3.cloudfront.net		13.224.94.20	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:41.356723070 CET	8.8.8.8	192.168.2.4	0xa59d	No error (0)	moremi.media		167.114.89.121	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:42.004729033 CET	8.8.8.8	192.168.2.4	0x31b	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:42.004729033 CET	8.8.8.8	192.168.2.4	0x31b	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:42.172002077 CET	8.8.8.8	192.168.2.4	0xc5d	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 02:39:42.172002077 CET	8.8.8.8	192.168.2.4	0xc5d	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Jan 14, 2021 02:39:42.191591978 CET	8.8.8.8	192.168.2.4	0xa12e	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 14, 2021 02:39:23.138312101 CET	13.224.94.31	443	192.168.2.4	49736	CN=*.typeform.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	Mon Nov 30 01:00:00 CET 2020	Thu Dec 30 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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		
Jan 14, 2021 02:39:23.138860941 CET	13.224.94.31	443	192.168.2.4	49737	CN=*.typeform.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	Mon Nov 30 01:00:00 CET 2020	Thu Dec 30 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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
Jan 14, 2021 02:39:24.218924046 CET	13.224.94.86	443	192.168.2.4	49740	CN=*.typeform.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	Mon Nov 30 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	Thu Dec 30 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		
Jan 14, 2021 02:39:24.296129942 CET	13.224.94.86	443	192.168.2.4	49739	CN=*.typeform.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	Mon Nov 30 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	Thu Dec 30 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 14, 2021 02:39:24.372504950 CET	13.224.94.88	443	192.168.2.4	49743	CN=*.typeform.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	Mon Nov 30 01:00:00 CET 2020	Thu Dec 30 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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		
Jan 14, 2021 02:39:24.373157978 CET	13.224.94.88	443	192.168.2.4	49744	CN=*.typeform.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	Mon Nov 30 01:00:00 CET 2020	Thu Dec 30 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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
Jan 14, 2021 02:39:25.325898886 CET	13.224.100.80	443	192.168.2.4	49747	CN=*.segment.com, O="Segment.io, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jun 12 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Tue Jul 27 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jan 14, 2021 02:39:25.328418016 CET	13.224.100.80	443	192.168.2.4	49748	CN=*.segment.com, O="Segment.io, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jun 12 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Tue Jul 27 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jan 14, 2021 02:39:25.492623091 CET	162.247.242.19	443	192.168.2.4	49745	CN=*.nr-data.net, O="New Relic, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 05 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Tue Feb 08 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jan 14, 2021 02:39:25.494162083 CET	162.247.242.19	443	192.168.2.4	49746	CN=*.nr-data.net, O="New Relic, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 05 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Tue Feb 08 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jan 14, 2021 02:39:26.062858105 CET	52.41.92.51	443	192.168.2.4	49749	CN=*.segment.com, O="Segment.io, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jun 12 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Tue Jul 27 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 14, 2021 02:39:26.316965103 CET	52.41.92.51	443	192.168.2.4	49750	CN=*.segment.com, O="Segment.io, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jun 12 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Tue Jul 27 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jan 14, 2021 02:39:41.629339933 CET	167.114.89.121	443	192.168.2.4	49758	CN=moremi.media CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US 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	Sat Dec 26 01:00:00 CET 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sat Mar 27 00:59:59 CET 2021 Sun May 18 01:59:59 CEST 2025 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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					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		
Jan 14, 2021 02:39:41.633831024 CET	167.114.89.121	443	192.168.2.4	49759	CN=moremi.media CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US 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	Sat Dec 26 01:00:00 CET 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sat Mar 27 00:59:59 CET 2021 Sun May 18 01:59:59 CEST 2025 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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					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		
Jan 14, 2021 02:39:42.096379995 CET	104.16.18.94	443	192.168.2.4	49762	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 14, 2021 02:39:42.097338915 CET	104.16.18.94	443	192.168.2.4	49763	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	Wed Oct 21 02:00:00 CEST 2020	Thu Oct 21 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 14, 2021 02:39:42.256901979 CET	152.199.23.37	443	192.168.2.4	49765	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020	Fri Jul 09 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jan 14, 2021 02:39:42.257751942 CET	152.199.23.37	443	192.168.2.4	49766	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020	Fri Jul 09 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jan 14, 2021 02:39:42.258147955 CET	152.199.23.37	443	192.168.2.4	49764	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020	Fri Jul 09 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

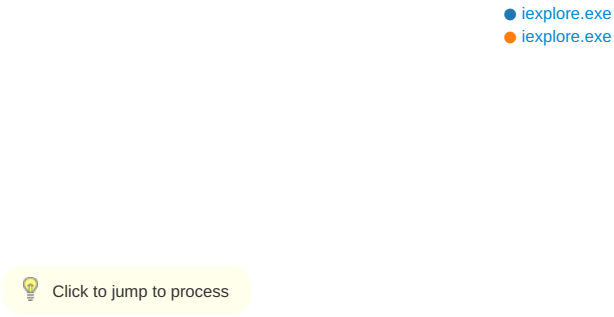
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jan 14, 2021 02:39:42.262120962 CET	152.199.23.37	443	192.168.2.4	49767	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jan 14, 2021 02:39:42.262824059 CET	152.199.23.37	443	192.168.2.4	49768	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jan 14, 2021 02:39:42.262938976 CET	152.199.23.37	443	192.168.2.4	49769	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 6912 Parent PID: 800

General

Start time:	02:39:19
Start date:	14/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff67a650000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
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

Copyright null 2021

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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: 6956 Parent PID: 6912

General

Start time:	02:39:20
Start date:	14/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6912 CREDAT:17410 /prefetch:2
Imagebase:	0xac0000
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

Copyright null 2021