ID: 345213
Cookbook: browseurl.jbs
Time: 20:41:51
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

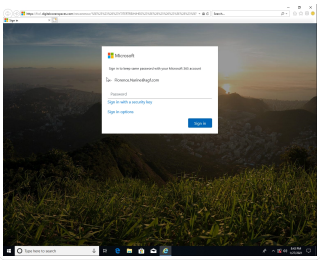
Analysis Report https://archchicago.us7.list-manage.co…

Overview

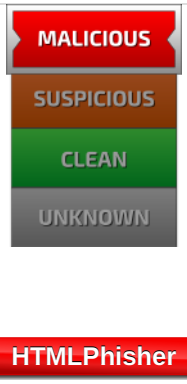
General Information

Sample URL:	http://https://archchicago.us7.list-manage.com/track/click?u=32277848bb5b49b8121a67d14&id=54644935c5&e=e7e099342b#Florence.Narine@agf.com
Analysis ID:	345213

Most interesting Screenshot:



Detection



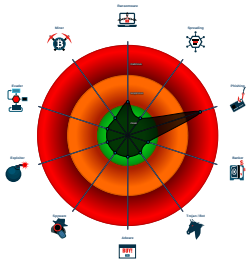
HTMLPhisher

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- Yara detected HtmlPhish_10
- Phishing site detected (based on log…
- Found iframes
- HTML body contains low number of …
- No HTML title found
- URL contains potential PII (phishing…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 4872 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1320 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4872 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

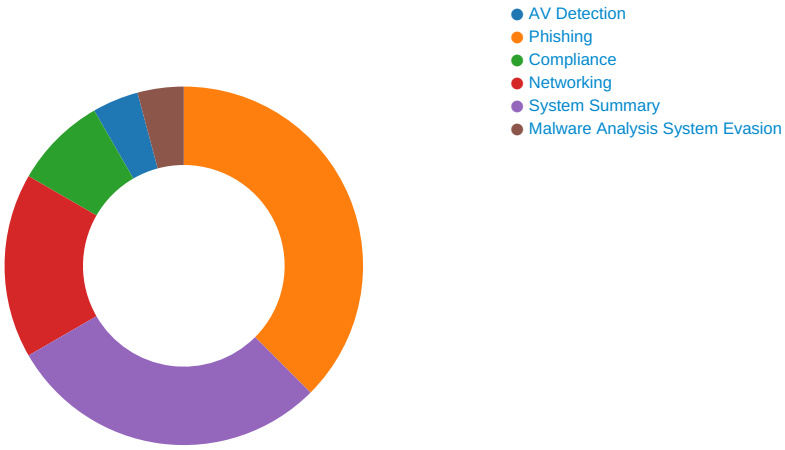
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\^%25#&#YTJTERTREJHJHEG#^&%25&#^(#^(#&(#^&#^#%25O(#&)(&##&([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:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish_10

Phishing site detected (based on logo template match)

Compliance:

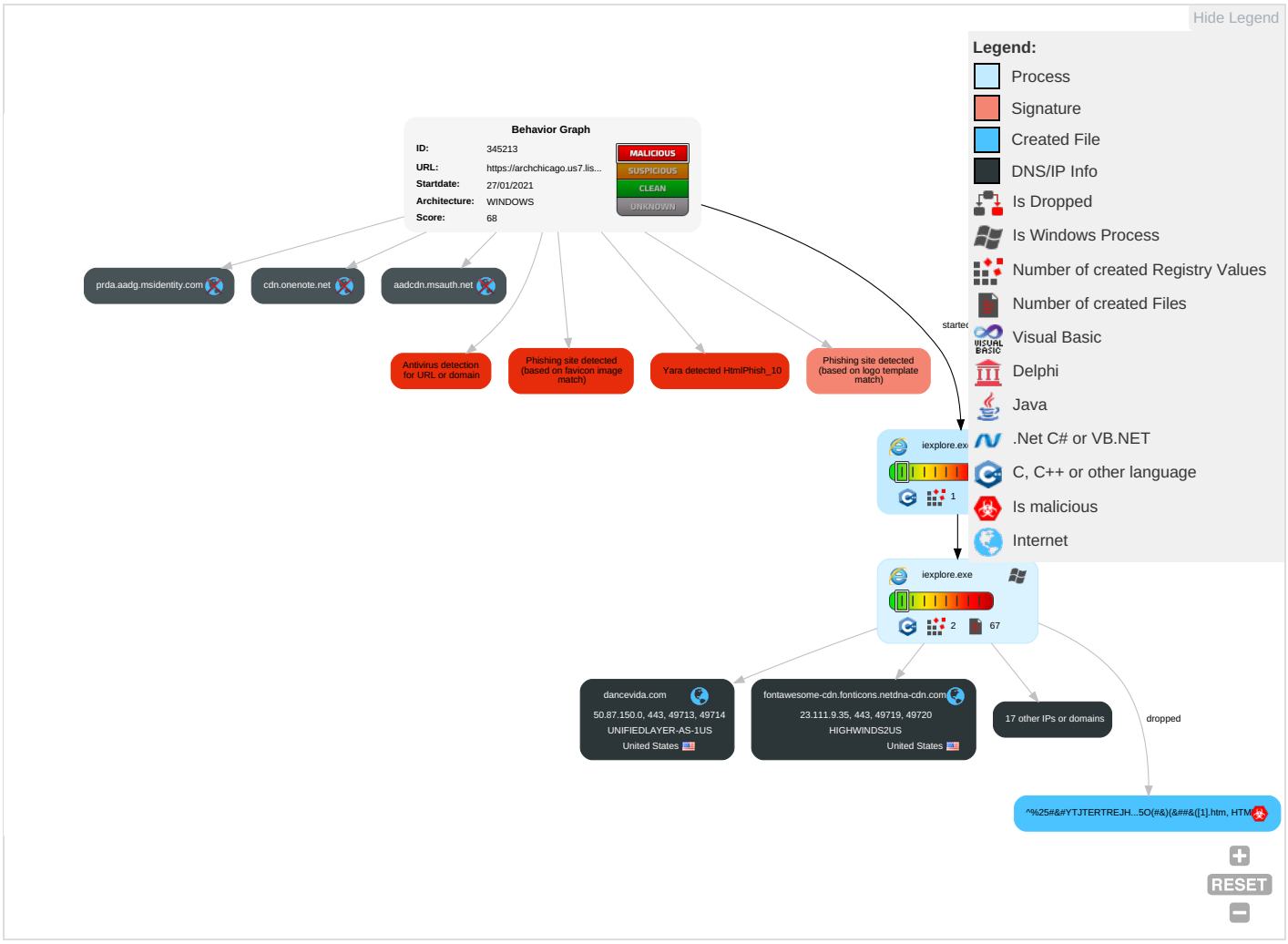
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Drive-by Compromise 1	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software 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
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	File and Directory Discovery 1	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
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

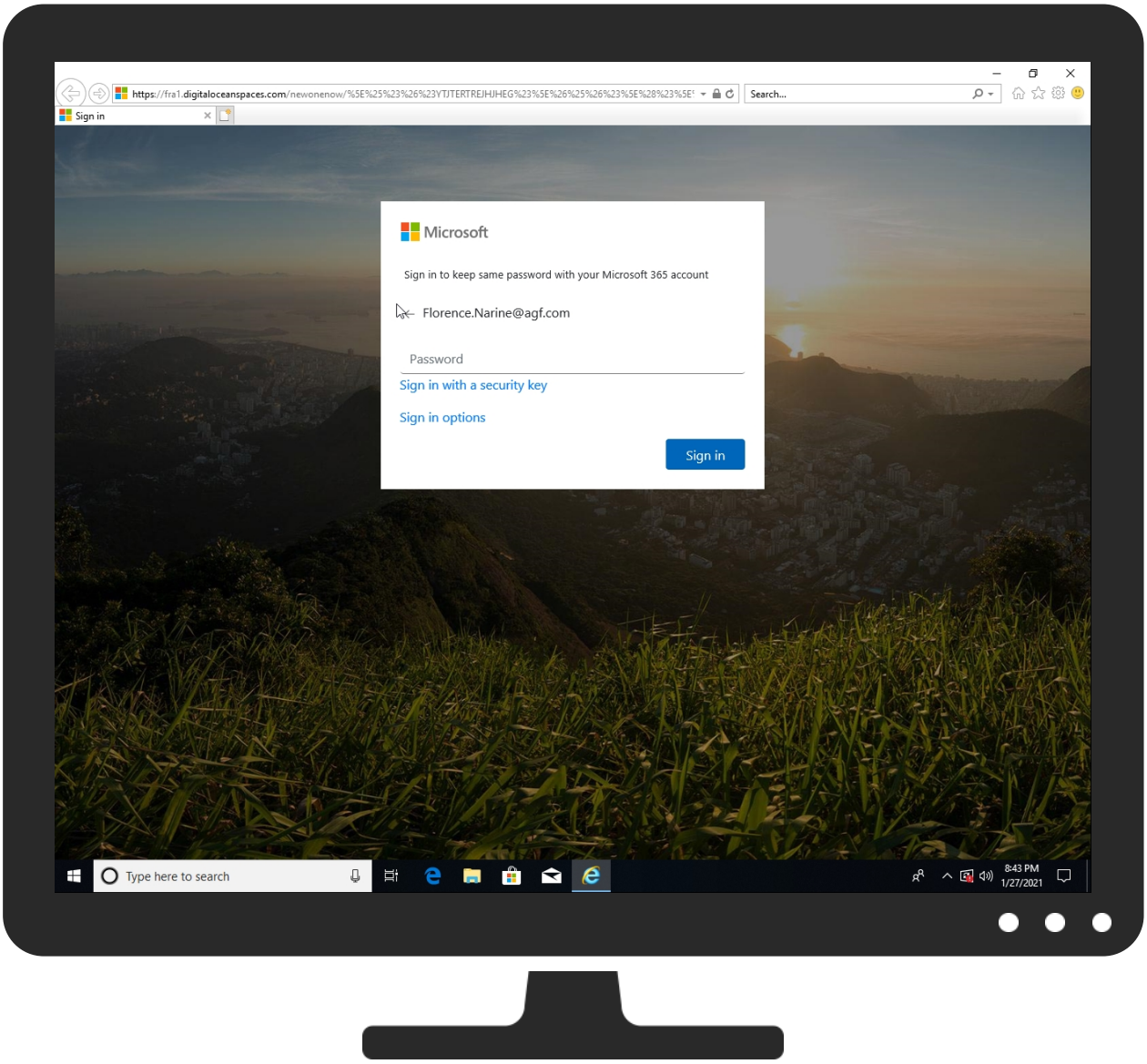
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://archchicago.us7.list-manage.com/track/click?u=32277848bb5b49b8121a67d14&id=54644935c5&e=e7e099342b#Florence.Narine@agf.com	0%	Virustotal		Browse
http://https://archchicago.us7.list-manage.com/track/click?u=32277848bb5b49b8121a67d14&id=54644935c5&e=e7e099342b#Florence.Narine@agf.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
dancevida.com	1%	Virustotal		Browse
cs1100.wpc.omegacdn.net	0%	Virustotal		Browse
sustainableinfrastructure.org	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://fra1.digitaloceanspaces.com/newonenow/%5E%25%23%26%23YTJTERTREJHJHEG%23%5E%26%25%26%23%5E%28%23%5E%28%23%26%28%23%5E%26%23%5E%23%25O%28%23%26%29%28%26%23%23%26%28.html#Florence.Narine@agf.com	100%	SlashNext	Fake Login Page type: Phishing & Social usering	
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/jquery.1.11.min_tu0oeunbyls-a4imj8e0xq2.js	0%	Avira URL Cloud	safe	
http://https://fra1.digitaloc	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~(	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~(	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~(	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/personal_account_0f72b5950600f24e7f9a604b186f3	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/work_account_1963c6b1926b773986f53f844ce4c32e.	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/microsoft_logo.png	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/aad.login.min_c38fti7z7e0m2csp02b-sa2.js	0%	Avira URL Cloud	safe	
http://https://dancevida.com/css/app.css	0%	Avira URL Cloud	safe	
http://gsgd.co.uk/sandbox/jquery/easing/	0%	URL Reputation	safe	
http://gsgd.co.uk/sandbox/jquery/easing/	0%	URL Reputation	safe	
http://gsgd.co.uk/sandbox/jquery/easing/	0%	URL Reputation	safe	
http://https://sms.baptemedelair.fr/vendor/todayzoo.php	0%	Avira URL Cloud	safe	
http://https://sustainableinfrastructure.org/wp-content/themes/isi-child/images/waiting.gif	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/backgrounds/0-small_138bcee624fa04ef9b75e86211	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000.28543.10/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc1937	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000.28543.10/content/images/backgrounds/0_a5dbd4393ff6a725c7e62b61df7	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/backgrounds/0_a5dbd4393ff6a725c7e62b61df7e72f0	0%	Avira URL Cloud	safe	
http://https://www.orka.mk/consdidews32ewdsering/pdansdidewsd32waedsrish?ct=t(Parish_Food_Pantry_1_26_2021_	0%	Avira URL Cloud	safe	
http://https://fra1.digitalocnsdidews32ewdsering/pdansdidewsd32waedsrish?ct=t(Parish_Food_Pantry_1_26_2021_	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dancevida.com	50.87.150.0	true	false	• 1%, Virustotal, Browse	unknown
cs1100.wpc.omegacdn.net	152.199.23.37	true	false	• 0%, Virustotal, Browse	unknown
fra1.digitaloceanspaces.com	5.101.109.44	true	false		high
sustainableinfrastructure.org	3.218.111.133	true	false	• 0%, Virustotal, Browse	unknown
cdnjs.cloudflare.com	104.16.19.94	true	false		high
fontawesome-cdn.fonticons.netdna-cdn.com	23.111.9.35	true	false		high
cs1227.wpc.alphacdn.net	192.229.221.185	true	false		unknown
orka.mk	23.227.133.50	true	false		unknown
stackpath.bootstrapcdn.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
logincdn.msauth.net	unknown	unknown	false		unknown
aadcdn.msftauth.net	unknown	unknown	false		unknown
aadcdn.msauth.net	unknown	unknown	false		unknown
use.fontawesome.com	unknown	unknown	false		high
www.orka.mk	unknown	unknown	false		unknown
archchicago.us7.list-manage.com	unknown	unknown	false		high
login.microsoftonline.com	unknown	unknown	false		high
cdn.onenote.net	unknown	unknown	false		unknown

Contacted URLs

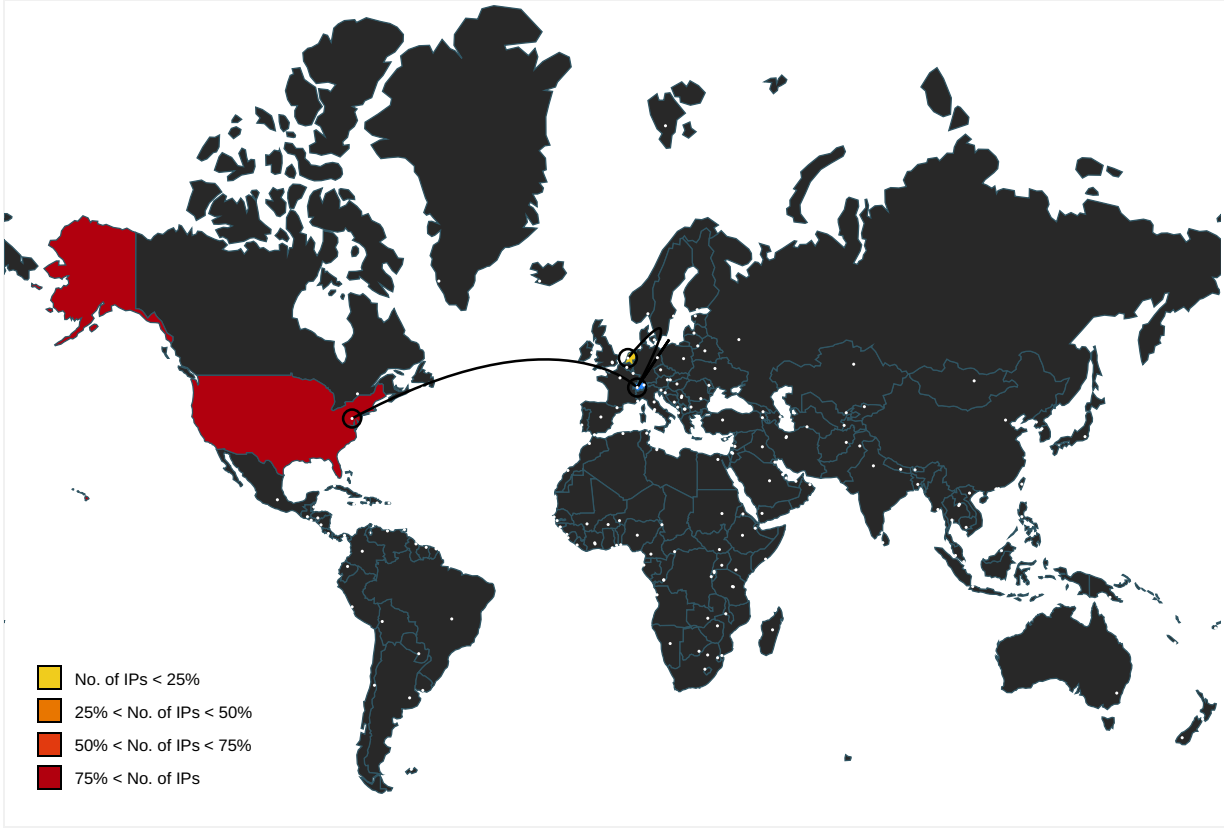
Name	Malicious	Antivirus Detection	Reputation
http://https://fra1.digitaloceanspaces.com/newonenow/	false		high
http://https://fra1.digitaloceanspaces.com/newonenow/%5E%25%23%26%23YTJTERTREJHJHEG%23%5E%26%25%26%23%5E%28%23%5E%28%23%26%28%23%5E%26%23%5E%23%25O%28%23%26%29%28%26%23%23%26%28.html#Florence.Narine@agf.com	false	• SlashNext: Fake Login Page type: Phishing & Social usering	high
http://https://fra1.digitaloceanspaces.com/newonenow/%5E%25%23%26%23YTJTERTREJHJHEG%23%5E%26%25%26%23%5E%28%23%5E%28%23%26%28%23%5E%26%23%5E%23%25O%28%23%26%29%28%26%23%23%26%28.html#	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js	^%25#&#YTJTERTREJHJHEG#^&%25&#^(#^(#&(#^&#^#%25O(#&)(&##&([1].htm.2.dr	false		high
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/jquery.1.11.min_tu0oeunbyls-a4imj8e0xq2.js	logout[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://fra1.digitaloc	{42C4481C-6123-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_aeupayfgghqiai7k9sol6lg2.ico	imagestore.dat.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fwdssp.com/?dn=referer_detect&pid=5POL4F2O4	suspendedpage[1].htm.2.dr	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css	^%25#&#YTJTERTREJHJHEG#^&%25&#^(#^(#&(#^&#^#%25O(#&)(&##&([1].htm.2.dr	false		high
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_aeupayfgghqiai7k9sol6lg2.ico~(	imagestore.dat.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/images/personal_account_0f72b5950600f24e7f9a604b186f3	logout[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/images/work_account_1963c6b1926b773986f53f844ce4c32e.	logout[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/images/microsoft_logo.png	logout[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js	^%25#&#YTJTERTREJHJHEG#^&%25&#^(#^(#&(#^&#^#%25O(#&)(&##&([1].htm.2.dr	false		high
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/aad.login.min_c38fti7z7e0m2csp02b-sa2.js	logout[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://fra1.digitaloceanspaces.com/newonenow/%5E%25%23%26%23YTJTERTREJHJHEG%23%5E%26%25%26%23%5E%28	~DFFC78C53105AF8248.TMP.1.dr	false		high
http://https://fra1.digitaloceanspaces.com/newonenow/E%25%23%26%23YTJTERTREJHJHEG%23%5E%26%25%26%23%5E%28%2	~DFFC78C53105AF8248.TMP.1.dr	false		high
http://https://github.com/douglascrockford/JSON-js	logout[1].htm.2.dr	false		high
http://https://getbootstrap.com/)	bootstrap.min[1].js.2.dr, bootstrap.min[2].js.2.dr, bootstrap.min[1].css.2.dr	false		high
http://https://dancevida.com/css/app.css	^%25#&#YTJTERTREJHJHEG#^&%25&#^(#^(#&(#^&#^#%25O(#&)(&##&([1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://fontawesome.com/license/free	all[1].css.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://gsgd.co.uk/sandbox/jquery/easing/	jquery.1.11.min_tu0oeunbyls-a4imj8e0xq2[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sms.baptemedelair.fr/vendor/todayzoo.php	^%25#&#YTJTERTREJHJHEG#^&%25&#^(#^(#&(#^&#^#%25O(#&)(&##&([1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://sustainableinfrastructure.org/wp-content/themes/isi-child/images/waiting.gif	^%25#&#YTJTERTREJHJHEG#^&%25&#^(#^(#&(#^&#^#%25O(#&)(&##&([1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://fontawesome.com	all[1].css.2.dr	false		high
http://https://aadcdn.msftauth.net/shared/1.0/content/images/backgrounds/0-small_138bcee624fa04ef9b75e86211	logout[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/twbs/bootstrap/graphs/contributors)	bootstrap.min[1].js.2.dr, bootstrap.min[2].js.2.dr	false		high
http://https://aadcdn.msauth.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://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.bundle.min.js	^%25#&#YTJTERTREJHJHEG#^&%25&#^(#^(#&(#^&#^#%25O(#&)(&##&([1].htm.2.dr	false		high
http://https://aadcdn.msauth.net/ests/2.1/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg	^%25#&#YTJTERTREJHJHEG#^&%25&#^(#^(#&(#^&#^#%25O(#&)(&##&([1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://logincdn.msauth.net/16.000.28543.10/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc1937	^%25#&#YTJTERTREJHJHEG#^&%25&#^(#^(#&(#^&#^#%25O(#&)(&##&([1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://use.fontawesome.com/releases/v5.6.1/css/all.css	^%25#&#YTJTERTREJHJHEG#^&%25&#^(#^(#&(#^&#^#%25O(#&)(&##&([1].htm.2.dr	false		high
http://https://logincdn.msauth.net/16.000.28543.10/content/images/backgrounds/0_a5dbd4393ff6a725c7e62b61df7	^%25#&#YTJTERTREJHJHEG#^&%25&#^(#^(#&(#^&#^#%25O(#&)(&##&([1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[1].js.2.dr, bootstrap.min[1].css.2.dr	false		high
http://https://login.microsoftonline.com/logout.srf?ct=1548343592&rver=64.4.6456.0&lc=1033&id=501392	^%25#&#YTJTERTREJHJHEG#^&%25&#^(#^(#&(#^&#^#%25O(#&)(&##&([1].htm.2.dr, {42C4481C-6123-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false		high
http://https://aadcdn.msftauth.net	logout[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	logout[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/images/backgrounds/0_a5dbd4393ff6a725c7e62b61df7e72f0	logout[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.orka.mk/consdidews32ewdsering/pdansdidewsd32waedsrish?ct=t(Parish_Food_Pantry_1_26_2021_	{42C4481C-6123-11EB-90E5-ECF4BB2D2496}.dat.1.dr, ~DFFC78C53105AF8248.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js	^%25#&#YTJTERTREJHJHEG#^&%25&#^(#^(#&(#^&#^#%25O(#&)(&##&([1].htm.2.dr	false		high
http://https://fra1.digitalocnsdidews32ewdsering/pdansdidewsd32waedsrish?ct=t(Parish_Food_Pantry_1_26_2021_	{42C4481C-6123-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.218.111.133	unknown	United States		14618	AMAZON-AESUS	false
23.111.9.35	unknown	United States		33438	HIGHWINDS2US	false
23.227.133.50	unknown	United States		55081	24SHELLSUS	false
192.229.221.185	unknown	United States		15133	EDGECASTUS	false
152.199.23.37	unknown	United States		15133	EDGECASTUS	false
5.101.109.44	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	false
50.87.150.0	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false
104.16.19.94	unknown	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345213
Start date:	27.01.2021
Start time:	20:41:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://archchicago.us7.list-manage.com/track/click?u=32277848bb5b49b8121a67d14&id=54644935c5&e=e7e099342b#Florence.Narine@agf.com
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:	4
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.phis.win@3/38@14/9
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://fra1.di gitaloceanspaces.com/newonenow /%5E%25%23%26%23YTJTERTREJHJHE G%23%5E%26%25%26%23%5E%28%23%5 E%28%23%26%28%23%5E%26%23%5E%2 3%25O%28%23%26%29%28%26%23%23% 26%28.html# • Browsing link: https://fra1.di gitaloceanspaces.com/newonenow/
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, ielowutil.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 104.108.39.131, 40.88.32.150, 23.50.105.71, 209.197.3.15, 13.107.246.13, 172.217.22.234, 20.190.159.136, 40.126.31.143, 40.126.31.1, 40.126.31.6, 40.126.31.139, 40.126.31.8, 40.126.31.137, 40.126.31.141, 104.108.60.202, 20.190.159.132, 20.190.159.138, 20.190.159.134, 93.184.220.29, 23.210.249.50, 152.199.19.161 • Excluded domains from analysis (whitelisted): storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, cs9.wac.phicdn.net, e13829.x.akamaiedge.net, www.tm.lg.prod.aadmsa.akadns.net, storeedgefd.xbetservices.akadns.net, www.tm.a.prd.aadg.trafficmanager.net, cdn.onenote.net.edgekey.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, ocsp.digicert.com, login.live.com, swc.list-manage.com.edgekey.net, watson.telemetry.microsoft.com, storeedgefd.dsx.mp.microsoft.com, aadcdnoriginwus2.azureedge.net, ajax.googleapis.com, ie9comview.vo.msecnd.net, lgincdnvzeuno.ec.azureedge.net, aadcdnoriginneu.azureedge.net, skypedataprdcolcus16.cloudapp.net, Edge-Prod-FRAr3.ctrl.t-0003.t-msedge.net, star-azureedge-prod.trafficmanager.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, login.msa.msidentity.com, lgincdnvzeuno.azureedge.net, aadcdnoriginneu.ec.azureedge.net, t-0003.t-msedge.net, lgincdn.trafficmanager.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, aadcdnoriginwus2.afd.azureedge.net, e1553.dspg.akamaiedge.net, cds.j3z9t3p6.hwcdn.net, e16646.dscg.akamaiedge.net, dub2.next.a.prd.aadg.trafficmanager.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\Recovery\High\Active\RecoveryStore.{42C4481A-6123-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8529563941287852
Encrypted:	false
SSDEEP:	192:rwZnZQu2QtL9WQtHqDtQtHqZsTfQtHqZKLDOyMQtHWyKAWSQtHWZZK1EYQtHWZZj:rgZUEUjQTgOzoWSJ8EYJHZJgRu
MD5:	212A7F9E34C94B707B242D00A83FAAF7
SHA1:	F58D2CCDA7E16668E03CA5F61EEE9023F2E4BD1B
SHA-256:	7ED1D6B26C618687BFDE698841A985846DF395CE7143E40BDA27A3D421551F7D
SHA-512:	3ADFBE60C58AD344569D7BCB07BCA80C8F2D94FACA565BEBE98C684DABF3609BD3959F02D41FF436DEAF2A7DB93B4667DF7CAD315398E5C3D10E0DF423DF234
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\{42C4481C-6123-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	69464
Entropy (8bit):	2.5395969378780303
Encrypted:	false
SSDEEP:	768:rfL05RLK5tuLc5tuLz5tuLT5tuLe5tuLU9z5tuLwVLK5tuULo5tuLB95tv5tuLIR:r4j
MD5:	8EF4C86634D437E45FD8F716D811668F
SHA1:	530F500DDF99F63790F7D036C4285708B4914A0B
SHA-256:	83F665F3C6E1EABB43E1E907E5FB3E6080E8B0977EF8950AF7E7591089BE7C01
SHA-512:	4ED088255F4CC19345491455E61FD23193007044B1A9A955FD4B2E293EE8BF7D519DCA06C74FF99610C4CCADAA01C5D6B4D8AB38333771943D351675B0D154F
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{42C4481C-6123-11EB-90E5-ECF4BB2D2496}.dat	
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y.. ....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{4A79DAA2-6123-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.563198001615345
Encrypted:	false
SSDEEP:	48:IwTGcpr+GwparG4pQLGrapbSorGQpKKG7HpRXsTGIpG:rpZ2Qt6/BSoFAlTX4A
MD5:	937BBB3C2B8F5EEEB182A370E6AFCF70
SHA1:	18BBDB60F78481F5D480E7DB4284A4C6BB8ECEF2
SHA-256:	4AF6F2FFBA2D4DB4E5ACADE919C0FD592FFA2FA99ACFE55AD08600B5CBC4EE39
SHA-512:	A155B353233CA1B6D9BDB9AD1444A1FF35C6690E21DBA535E58DBA3E6953D75DE1B32C2DCC4C602A4C7C6471AFC5D1DE628E2E4642963EB3705FDC8005318I 0A
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y.. ....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\wlm7n14\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	18476
Entropy (8bit):	3.1372025556582472
Encrypted:	false
SSDEEP:	48:sT5gT5FT5dT5YgyyyyyyyyyyyyydT5KYT5/QQQQQ5:+gTTIb9QQQQQ5
MD5:	91EDE062283FA787C92FC9D7F464346A
SHA1:	99830E255CC6F6015E164FAF4502CE8664C0B2B6
SHA-256:	29AE2FED3113F563770FD41FCAB7E946412FD0A3922C73B3A0EB9A0182DBDDD2
SHA-512:	500A9605D62D1C209671AC1611A4F8B102A0AD9941B2F0EC14DC46FADE7B747C378374B24D88E433D6C8D8250BD36B142CD1006E172700CA95E6FC44E6B96C8
Malicious:	false
Reputation:	low
Preview:	W.h.t.t.p.s.:././.a.a.d.c.d.n...m.s.a.u.t.h...n.e.t./.e.s.t.s./.2...1./.c.o.n.t.e.n.t./.i.m.a.g.e.s./.f.a.v.i.c.o.n._.a._.e.u.p.a.y.f.g.g.h.q.i.a.i.7.k.9.s.o.l.6.l.g.2...i.c.o.~(................h(......(....... ....(.....................................''P..'' ...3333333333333333333333333333333'' ...3333333 333333333333333333333333'' ...3333333333333333333333333333333'' ...3333333333333333333333333333333'''''''''''' '''''''''''''''''''''''''''' ...3333333333333333333333333333333'' ...3333333333333333333333333333333'' ...3333333333333333 3333333333333'' ...3333333333333333333333333333333'' ...3333333333333333333333333333333'' ...3333333333333333333333333333333'' ...33333333333333333333

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\aad.login.min_c38fti7z7e0m2csp02b-sa2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	180385
Entropy (8bit):	5.426784882698052
Encrypted:	false
SSDEEP:	1536:/SjqwT+zx4Nm7t21ikgDy8k8tvnytWoULhn92gMNCBfLmt1kX0qIhvsGKytp2:/cp+14S2zshqkT81C9GKW2
MD5:	737F054E2ED9EC4D0CD824A9D3607E48
SHA1:	872F05E28C305DAF3412ADD6D2A2092934BAC847
SHA-256:	6B5057E112FA77F6C48B736E66D210A22BB097BA89A93B3D5BF76C51C95EFAD5
SHA-512:	7314BA83F529D74CC637B85C7E67A57B7D994C11B167DE1880DE55602D1C901FAA3323550DF117F163237581770B39B504A7CA18D701BEC149028AF5999BDE40
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/aad.login.min_c38fti7z7e0m2csp02b-sa2.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\aad.login.min_c38fti7z7e0m2csp02b-sa2[1].js	
Preview:	/*! --- START OF THIRD PARTY NOTICE ---..This file is based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise. .. * json2.js (2016-05-01). * https://github.com/douglascrockford/JSON-js. * License: Public Domain..Provided for Informational Purposes Only..Public Domain. .NO WARRANTY EXPRESSED OR IMPLIED. USE AT YOUR OWN RISK..----------END OF THIRD PARTY NOTICE --- */."object"!=typeof JSON&&(JSON={}),

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\http_403[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4585
Entropy (8bit):	4.046190045670235
Encrypted:	false
SSDEEP:	48:upUw1V4VOBXvLwSZIPTC5f1a5TI7jn3GFa7KGuc1kpNc7K1rfQy:u3p9ZQw6Kj36a7gG7I
MD5:	3215E2E80AA8B9FABA83D76AEF71F1B9
SHA1:	C7582D414EE6A1DAE098F6DBBBF68ED9641D0023
SHA-256:	D91C22EF6451561F346B8C8BC6F98897E2E5C28135A421EE946800F6C8451B24
SHA-512:	690E4D62229AD14D3D842DABE986651B4CC2E4C873A50E5B7FC4FD539662A703690ECC70649ACEA7751E69CE6046489C0E6B05D24F0030D68773C67B3DCBAE0
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/http_403.htm
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html>.... <head>.. <link rel="stylesheet" type="text/css" href="ErrorPageTemplate.css" />.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>.... <title>HTTP 403 Forbidden</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:expandCollapse('infoBlockID', true); initGoBack(); initMoreInfo('infoBlockID');">.... <table width="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" width="60" align="left" valign="top" rowspan="2">.. <img src="info_48.png" id="infoIcon" alt="Info icon">.. </td>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC134
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/info_48.png
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po.....X..;.=.P...../...+...9./..s.....9..|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0..''/n/.c...&.{.ht..?....A..I{.n.....|....t.....N}..%.v...:.E..i....`....a.k.mg.LX..fcFU.fO-..YEfd.}...~.''.....}!$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a...N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a)..t..e.j.W.....C<.1.....c..l1w....]3%....tR;,..3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\microsoft_logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 108 x 24, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1057
Entropy (8bit):	7.6851406288304105
Encrypted:	false
SSDEEP:	24:Qb0EcwtZDFHs70yTIy9pEq0WVBtXVMDug3iLRciNe47zz:QIEFA7pdl3tFEWRRPz
MD5:	ED9C9EB0DCE17D752BEDEA6B5ACDA6D9
SHA1:	ECA56C4904354EED5DA0DEBCD6BD66856AB4784D
SHA-256:	F664B8138C2DA6EC7565500A7CC839DA6372614A31DC04C5A2169A26B8D9767C
SHA-512:	3BFB696318DDB93540140DBCD4DBB32F129441E46EE752C6B7379624488533BA27CC7EFF3CAE444C1797CA6EECDF333EDAF443AC84CDEB037A890967091CF9C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\microsoft_logo[1].png	
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/microsoft_logo.png
Preview:	.PNG.....IHDR...I.....pHYs.....~.....IDATh..XMN.P..\.E.....' ,.-.$'.H....s...1.vQ.....4.....-.<.....{..|.?.w[4....A.=h<>.....7..t.u..]A{..&...,..h.`D4.01].....H.&..C.w. ..@....*..a..3..H.aR.=.g.(.0.6...;Wl...X.X..G.Bf.....D4...K..p... ..hh.-b.R.Z....Z..zYQc}....u^..R.Dzm$..%c".....C.*z.\&U9P..0.3s*..31..@...W..2....yG.....c)k.F....3.I!....2..F.... .`%1.....-..U.s(.p..S.($/...}(.5.\"k.+.I.Q...cb....kt..o.`.....%L....;.J.[..b.xx)c,X7.....)..'.n..H=E<.B.].g.}f.o.....znJ.....Q$....7...#.&..g.D..X....F..~=...%IQ.....e.....>.R.....s.. [.D|.n&..a06..d.5.5YGC..3N.....<..Pt..\<{b...i.....)!.....8...0.t_.....8..T.....)G.-mzK...../..TDK..k..s"ch.0....i..`...`V..H.Q"...x.....!.."..Q..%3O.L.....$....e.s.m..|.....AD."...#.%b,'..r!.}c ...X!2kCD6..iX.\@S..3Er....B...D...%.O...(._...-....{b.....z.....r.N..W2....L.1~-.J.?.l....?..q:..W.5&.....|..>.B...G.oa.S.....1.....Zo...q.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\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://logincdn.msauth.net/16.000.28543.10/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-.39,1.392, 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\3Y2ADQKS\suspendedpage[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	494
Entropy (8bit):	4.962239405540505
Encrypted:	false
SSDEEP:	12:hnMQbwzRQ6QclfhxxEdWr+YZrH3atJMlgOt0quoQL:hMxRQspxCQnZrH3atEx0h
MD5:	0357AA49EA850B11B99D09A2479C321B
SHA1:	41472BA5C40F61FA1C77C42CF06248F13B8785F0
SHA-256:	0FF0B7FCB090C65D0BDCB2AF4BBD2C30F33356B3CE9B117186FA20391EF840A3
SHA-512:	A317A0F035B8DFF7CA60C76B0B75698A3528FD4C7C5E915292C982D2B38C1C937C318362C891E93BEE6FDB1B166764D7183140A837FD23DAA2BE3D2DAC5A5D C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dancevida.com/cgi-sys/suspendedpage.cgi
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">.<html>. <head>. <title>Contact Support</title>. <meta http-equiv="Conten t-Type" content="text/html; charset=utf-8">. </head>. <body marginwidth="0" marginheight="0" leftmargin="0" topmargin="0">. <iframe width="100%" height="100%" frameborder="0" SCROLLING="auto" marginwidth="0" src="http://fwdssp.com/?dn=referer_detect&pid=5POL4F2O4"></iframe>. </body>.</html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\waiting[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 256 x 256
Category:	downloaded
Size (bytes):	26990
Entropy (8bit):	7.888854974250368
Encrypted:	false
SSDEEP:	384:OQDneVCxzGNpIQjqhgNqlBJ4V8DqpLlwZeyWEjLfYBU8uslUOVgl/tqb76BnuB8h:OhTpI6afixPZRQBUpVdP6Bnuqzr5
MD5:	8264C9B1C336082653C05481ECA90351
SHA1:	F88FF5D34B144109BF952FA0D039A76204150974
SHA-256:	D8EFFEED907DB567F755D4D20995E5728171EA06239BF0A56B48BB4C3830F66E
SHA-512:	2B271530819F25FB39A5EDFA17E03BC465F70603717AB74277319E1678005C4B77ADFAD4011520F38F059D8C2914CDE057DD50856FF690A6634770896843ADAC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sustainableinfrastructure.org/wp-content/themes/isi-child/images/waiting.gif

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\waiting[1].gif	
Preview:	GIF89a.....,....d.....L.....t..<.....t.....T.....l.....4..l.....|..D.....\..,....d.....L.....<.....|.....\.....!..NETSCAPE2.0.....!.....-.,.....pH,...r.l:.....y....4..z..xL....).}....|N...x.f..`..}{y.....^*|~..}.....e$.....X.$....s%.....J.....S..(.....l.#....r....._.....l.....`y.....^..@.....*T.p.P9.X.!..D.....$HP!....F`.. ..K#'N...,...v..."....-b.f.g..4W.....z *.9P..@~Vy1.).i..S{.G....).....!.$...!...s).K.....F.!AB....L.`<.....QH.NT...(P..T..x+...Y.....Kp`..w0.....$.....dfC.x;O....l.3.6-G.L.G.&.N,!,.f\ .#.2...?..&...@.....-X(.<.....w_~!....aD..;.u.... X....b.w"..`.....J..._.!@.....a.....8FLk...v2....,.8Bp:.../#...)}H...Lvq@.."9..MV...S<v.U..P..`6.`..$.X?&....a....!. g.n...}..(..|....*..j.&..6. .F*.Vji.Q.(.6.L..l....%q.....*Z..FJW'@.*S!...&..:.K..3M.....r..4.%+G.....p...'LR.A.:k.}..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\0-small_138bcee624fa04ef9b75e86211a9fe0d[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 50x28, frames 3
Category:	downloaded
Size (bytes):	3006
Entropy (8bit):	3.009694812062996
Encrypted:	false
SSDEEP:	12:tWK1TbpOMo7FL2cDPilY1Qtc150XyoseAfQx9Jq4U3DXCFSAt78aULgf5GY48:AK1hNo7FCWwNtc1spAYx9VOCUiXVf5x
MD5:	138BCEE624FA04EF9B75E86211A9FE0D
SHA1:	23BBCDAAEBD6C9A6E57E96E44493B2212860FCAB
SHA-256:	F89E9082807918O3BBF1F33B596FF4A2179B355A8E15AD02EBAA2B1DA11127EA
SHA-512:	D20765E5738F4AC5A91396B5F5D88057C3B5125840BCE42039AC9D5D75B1C3FB9629ACA6290A475625DFE60887CF59D4FB52108D024FF4FA8094C9B8458F9F33
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/shared/1.0/content/images/backgrounds/0-small_138bcee624fa04ef9b75e86211a9fe0d.jpg
Preview:	.....JFIF.....H.H.....Phttp://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c142 79.160924, 2017/07/13-01:06:39 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about=""/> </rdf:RDF> </x:xmpmeta>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\all[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	53741
Entropy (8bit):	4.712987947440229
Encrypted:	false
SSDEEP:	768:WVV316z1MPq4lQuUY3HJgkQCZ/mMQyjJKp7CzuNnQz8:WVizGC4lvxH6BCQgu7cumY
MD5:	B8085BF2C839791244BD95F56FB93C01
SHA1:	9D272F6A226ADC587B4C3E470CC146EDD8C92F75
SHA-256:	453893F7DAA3D8FE9716F8C6D0F36F8ADE8CACFC0093E164F4F998B46427959E
SHA-512:	071423C79D846BFB1A9CA8C9E36E8F021C5027804F7DA86249BFE886D67622982B739C326934A04F03E1859FF10BAEAFBE0F8DE2AA030F58F455C240A814E385
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.fontawesome.com/releases/v5.6.1/css/all.css
Preview:	/*!. * Font Awesome Free 5.6.1 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */..fa,.fab,.fal,.far,.fas{-moz-osx-font-smoothing:grayscale;-webkit-font-smoothing:antialiased;display:inline-block;font-style:normal;font-variant:normal;text-rendering:auto;line-height:1}.fa-lg{font-size:1.33333em;line-height:.75em;vertical-align:-.0667em}.fa-xs{font-size:.75em}.fa-sm{font-size:.875em}.fa-1x{font-size:1em}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-6x{font-size:6em}.fa-7x{font-size:7em}.fa-8x{font-size:8em}.fa-9x{font-size:9em}.fa-10x{font-size:10em}.fa-fw{text-align:center;width:1.25em}.fa-ul{list-style-type:none;margin-left:2.5em;padding-left:0}.fa-ul>li{position:relative}.fa-li{left:-2em;position:absolute;text-align:center;width:2em;line-height:inherit}.fa-border{border:.08em solid #eee;border-radius:.1em;padding:.2em .25em .15em}.fa-pull-lef

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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.msauth.net/ests/2.1/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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\9QTQHWWN\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	downloaded
Size (bytes):	453
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi
MD5:	20F0110ED5E4E0D5384A496E4880139B
SHA1:	51F5FC61D8BF19100DF0F8AADAA57FCD9C086255
SHA-256:	1471693BE91E53C2640FE7BAEECBC624530B088444222D93F2815DFCE1865D5B
SHA-512:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5A
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/background_gradient.jpg
Preview:	......JFIF.....d.d......Ducky.......P.......Adobe.d..... ....W..... .....Qa.....?.....%.....x.....s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\converged.v2.login.min_rayhgcterrtxpnvapp3erg2[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	107668
Entropy (8bit):	5.291456416114907
Encrypted:	false
SSDEEP:	1536:QpHDglkuhw+ExiazA/PWrF7qvEAFiQcpmWGQvz6yVUn1:lEJ4yVU1
MD5:	440CA18024DE46B4D73E7540A4FDDE46
SHA1:	C4FF7AF4E1558E081DF52C1E61A5D63D0BE577C7
SHA-256:	EA6449D448A48495C557755AF39701567925CEAFC30E06FBA05F65E723C91AA3
SHA-512:	3A3A9D58E0E9645E2399CD83F53D842CBA47AA42EBAFECAB9AE29784AA7CE8A842F0CE89DFE8E35E3CD7387ADCFB66DA68BFCD2EDCAE9560C5E9F775A7703B37
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/converged.v2.login.min_rayhgcterrtxpnvapp3erg2.css
Preview:	/*! Copyright (C) Microsoft Corporation. All rights reserved. *//*!.---------- START OF THIRD PARTY NOTICE ----------..This file based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise...//----------.twbs-bootstrap-sass (3.3.0).//----------..The MIT License (MIT)..Copyright (c) 2013 Twitter, Inc..Permission is hereby granted, free of charge, to any person

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\httpErrorPagesScripts[1]	
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\jquery.1.11.min_tu0oeunbyls-a4imj8e0xq2[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):	111908
Entropy (8bit):	5.327106347218457
Encrypted:	false
SSDEEP:	1536:3/i4ovK5ICx1GFNFnfzFUbx+rvih7GTAmIIyRslnMBkQRiUrJ+b3E64ZyRxRZZpG:P2uBmdlkRZ5oFeRh/h
MD5:	4EED281149DBCA5B3E6B820C8FC1345D
SHA1:	FDC2C0D2434BC6F15AD837A07437EB9A67F12BB6
SHA-256:	2AE2A2707694A024731738FF4D822FCBD54B7EF7FEF876E8F39F23A64B2EA218
SHA-512:	1E39CD3B7FA2889380755CBFE26DCB120455F91B9F1928AEC8866764EF5CC7E5EE769458E4474739FE9701D64D694128C5EEE11EB751B4416895006336CE391C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/jquery.1.11.min_tu0oeunbyls-a4imj8e0xq2.js
Preview:	/*! jQuery v1.11.2 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */.!function(e,t){"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(e){if(!e.document){throw new Error("jQuery requires a window with a document")}return t(e)}:t(e)}("undefined"!=typeof window?window:this,function(e,t){function n(e){var t=e.length,n=ie.type(e);return"function"!==n&&!ie.isWindow(e)&&(!(1!==e.nodeType||!t)||("array"===n||0===t||"number"==typeof t&&t>0&&t-1 in e))}function r(e,t,n){if(ie.isFunction(t)){return ie.grep(e,function(e,r){.return!!t.call(e,r,e)!==n})}if(t.nodeType){return ie.grep(e,function(e){return e===t!==n})}if("string"==typeof t){if(fe.test(t)){return ie.filter(t,e,n)}t=ie.filter(t,e)}return ie.grep(e,function(e){return ie.inArray(e,t)>=0!==n})}function i(e,t){do{e=e[t]}while(e&&1!==e.nodeType);return e}function o(e){var t=be[e]={};return ie.each(e.match(ye)||[],function(e,n){t[n]=!0}),t}function a(){he.addEventListener?(he.rem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	86927
Entropy (8bit):	5.289226719276158
Encrypted:	false
SSDEEP:	1536:jLiBdiaWLOczCmZx6+VWuGzQNOzdn6x2RZd9SEnk9HB96c9Yo/NWLbVj3kC6t3:5kn6x2xe9NK6nC69
MD5:	A09E13EE94D51C524B7E2A728C7D4039
SHA1:	0DC32DB4AA9C5F03F3B38C47D883DBD4FED13AAE
SHA-256:	160A426FF2894252CD7CEBBDD6D6B7DA8FCD319C65B70468F10B6690C45D02EF
SHA-512:	F8DA8F95B6ED33542A88AF19028E18AE3D9CE25350A06BFC3FBF433ED2B38FEFA5E639CDDFDAC703FC6CAA7F3313D974B92A3168276B3A016CEB28F27DB0714A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Preview:	/*! jQuery v3.3.1 | (c) JS Foundation and other contributors | jquery.org/license */.!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery requires a window with a document");return t(e)}:t(e)}("undefined"!=typeof window?window:this,function(e,t){"use strict";var n=[],r=e.document,i=Object.getPrototypeOf,o=n.slice,a=n.concat,s=n.push,u=n.indexOf,l={},c=l.toString,f=l.hasOwnProperty,p=f.toString,d=p.call(Object),h={},g=function e(t){return"function"==typeof t&&"number"!=typeof t.nodeType},y=function e(t){return null!=t&&t===t.window},v={type:!0,src:!0,noModule:!0};function m(e,t,n){var i,o=(t=t||r).createElement("script");if(o.text=e,n)for(i in v)n[i]&&(o[i]=n[i]);t.head.appendChild(o).parentNode.removeChild(o)}function x(e){return null==e?e+"":"object"==typeof e||"function"==typeof e?l[c.call(e)]||"object":typeof e}var b="3.3.1",w=function(e,t){return new w.fn.init(e,t)},

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\logout[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, LF line terminators
Category:	dropped
Size (bytes):	441355
Entropy (8bit):	5.571717844719712
Encrypted:	false
SSDEEP:	3072:uSb++BAEJ4yVUx2uBmdlkRZ5oFeRh/Ucp+14S2zshqkT81C9GKW/Y:uS6+rislw3R6c426B8RY
MD5:	DC6D5F45DAA20ECE6A90A001045D0618
SHA1:	EEBD596D8920A7D20FA57A2116F080F9EB151DBC
SHA-256:	17F6B8A8B690DCCB145A7570F2C54733E71220F3B487ED609C398CCDD1A087F7
SHA-512:	B1388A657861A565C70ABC6FFA73BD687F9940B90EE992E2E517CA4946580CEA735F80F750EF8400662C617260AFA0D20E0C7BC5051F79C396278785844C00B4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\logout[1].htm	
Preview:	....<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">..<html dir="ltr" lang="en">..<head>.. .. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <meta http-equiv="X-UA-Compatible" content="IE=edge">.. <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=2.0, user-scalable=yes">.. <meta http-equiv="Pragma" content="no-cache">.. <meta http-equiv="Expires" content="-1">.. <link rel="preconnect" href="https://aadcdn.msftauth.net" crossorigin>..<meta http-equiv="x-dns-prefetch-control" content="on">..<link rel="dns-prefetch" href="//aadcdn.msftauth.net">..<link rel="dns-prefetch" href="//aadcdn.msauth.net">.... <meta name="PageID" content="signout" />.. <meta name="SiteID" content="" />.. <meta name="ReqLC" content="1033" />.. <meta name="LocLC" content="en-US" />.... ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\0_a5dbd4393ff6a725c7e62b61df7e72f0[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, baseline, precision 8, 1920x1080, frames 3
Category:	downloaded
Size (bytes):	283351
Entropy (8bit):	7.975896455873056
Encrypted:	false
SSDEEP:	6144:hPgRhluS12CyK8XGsLzsr5XONnQ4/bEmhZSlj6xU2zyOX/:2vz1pyWsLoXqN/YWPUU2OOX/
MD5:	A5DBD4393FF6A725C7E62B61DF7E72F0
SHA1:	55B292F885FFC92ABCE18750B07AA4ACFA4E903E
SHA-256:	211A907DE2DA0FF4A0E90917AC8054E2F35C351180977550C26E51B4909F2BEB
SHA-512:	850586A05B67EF25492BD50A090F1EC0A0CC21DC4E4EFEB35E19CDC78A98F9415A3807318FA02664EADE87F0E2D8FA2A2958CD0D712329800FC05689E01DC61
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://logincdn.msauth.net/16.000.28543.10/content/images/backgrounds/0_a5dbd4393ff6a725c7e62b61df7e72f0.jpg
Preview:	.....Phttp://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c142 79.160924, 2017/07/13-01:06:39 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about=""/> </rdf:RDF> </x:xmpmeta>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\ErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/ErrorPageTemplate.css
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_gradient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...background-color: #F4F4F4;..}.. ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	155758
Entropy (8bit):	5.06621719317054
Encrypted:	false
SSDEEP:	1536:b/xImT+IcCQYYDnDEBi83NcuSEk/ekX/uKiq3SYiLENM6HN26F:b/Riz7G3q3SYiLENM6HN26F
MD5:	A15C2AC3234AA8F6064EF9C1F7383C37
SHA1:	6E10354828454898FDA80F55F3DECB347FD9ED21
SHA-256:	60B19E5DA6A9234FF9220668A5EC1125C157A268513256188EE80F2D2C8D8D36
SHA-512:	B435CF71A9AE66C59677A3AC285C87EA702A87F32367FE5893CF13E68F9A31FCA0A8D14F6A7D692F23C5027751CE63961CA4FE8D20F35A926FF24AE3EB1D4B3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\bootstrap.min[1].css	
Preview:	/*!. * Bootstrap v4.3.1 (https://getbootstrap.com/). * Copyright 2011-2019 The Bootstrap Authors. * Copyright 2011-2019 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--orange:#fd7e14;--yellow:#ffc107;--green:#28a745;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--primary:#007bff;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;--warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoint-xl:1200px;--font-family-sans-serif:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,"Noto Sans",sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol","Noto Color Emoji";--font-family-monospace:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monospace}*,::after,::before{box-sizing:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\bullet[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKIv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/bullet.png
Preview:	.PNG........IHDR...............ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q.<..aw.<..dz.E...........1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.........z`....#tRNS................................./,....mIDATx^..C..`.......S....y'...05...|..k.X......*`.F.K....JQ..u.<.}.. ..[U..m....'r%.......yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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:QSNTmTFxg4lyyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsLsQZp:nfgyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico
Preview:	..............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(...................(.................................."P...""" ...3 333333333333333333333333333333""" ...333333333333333333333333333333""" ...333333333333333333333333333333"""" """"""""""""""""""""""""""""""""""""" ...333333333333333333333333333333""" ...333333333333333333333333333333""" ...33333333333 3333333333333333333""" ...333333333333333333333333333333""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""" """"""""" ...333333333333333333333333333333""" ...333333333333333333333333333333""" ...333333333333333333333 333333333""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\personal_account_0f72b5950600f24e7f9a604b186f3945[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 51 x 51, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1335
Entropy (8bit):	7.809886216220315
Encrypted:	false
SSDEEP:	24:vs/6B+yGr5mzV6gPxDMaanjZ9f/meF682olDYLTvprJ4kivLMEC8Awcrkrow6BBg:vs/6B+yGNmR2nTZ682olDkP493C8IrdU
MD5:	0F72B5950600F24E7F9A604B186F3945
SHA1:	3CCAF80771C291CC03FACD493F8EE9C03F1F238D
SHA-256:	0B874F4CCFAC9FF5264F1F7C29C4C016FDE7E4E032512BAC1BB43D145A44EA40
SHA-512:	E74F9D8080EA1C708E3AB48518ED58C9522B45E07EEAEB9B49F7B86922A7B16743E98EED13540F3362EE8A274680E0B807927FF6A83FD4D908F34EAB2C5912CD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/shared/1.0/content/images/personal_account_0f72b5950600f24e7f9a604b186f3945.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\personal_account_0f72b5950600f24e7f9a604b186f3945[1].png	
Preview:	.PNG.....IHDR...3...3.....:.0*....pHYs.....tEXtSoftware.Adobe ImageReadyq.e<....IDATx..Mh.A..'i.....U.).Ah.{..Y/^.Oz.....e{.c.7.G=..^*.B{..(V..&B.....g6...ffv....!d7.....M....].z.6....,..5aTa..x..Z.h.T\..(....c\.....5.....,.E..(.2...j....B.0.....j...@..."G..:z.....$.Bh.>....y.^l._..".-."a...rN..3...p..]....@[X1..BaTA..!R.1F..#.3.;$.....(.....'.w.B!...g.H.....0....Z.eA*...,.V..c.l7H../.....7....|.....@v$.m.U.F.....^]j.RX.....M....4Kw...1..N,....".V;....;?..?..>CEbQ.j.....]....z..v(..&....,L...@.d%J.K..w.R..@...=..`.?04W..W*....nb.q..yG...U....{.R....N..6C..&+..A0....C.j..X..,O#....8.)3....~..L..SY,....:).*._.....!..J5...z.+..f..Ly.[..A.....,....s.LF......?..H.'v>+|.6lV...F...}.t../..t?.].m.n.B..zg..U.r. U...y.&....e~rLl;;... ....r.........a...#b+.Z.g..u].=Pk..o....d.t...L..&+.(}...c...f.[H......B.....'_xp....E.k..%..8...j),;MU.....nw[a2.....8....(..X.......P1..R...8...MTQ9W.LE.L....".U...)....7.o.J.n.@.I...Z.^.d.L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\work_account_1963c6b1926b773986f53f844ce4c32e[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 51 x 51, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1487
Entropy (8bit):	7.8226450459839585
Encrypted:	false
SSDEEP:	24:vs/6BxHVamrbqZUh1HA0W7AckTifnHCW6mh7mC7ZPb0SCZJra8OkHLkf0f3a:vs/6BxHVaabqZUhVTBW9hb7ZgSKrlNLg
MD5:	1963C6B1926B773986F53F844CE4C32E
SHA1:	1324FA13FB62D6DCCDCFA258F205C01DA41409B7
SHA-256:	9FC929BE7892B2F4498627D22BC1B3990DC380EFCFE40FE6C3CAC2DEA7565C8E
SHA-512:	4120AEEA336993EC886F901492E7D5CC27304B8A095F6901EAEA8430CAAD10440B06E1FD60D63F78BA256BD8B26A32D62CD4F4FF0F1450195279EF243E0FC31
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/shared/1.0/content/images/work_account_1963c6b1926b773986f53f844ce4c32e.png
Preview:	.PNG.....IHDR...3...3.....:.0*....pHYs.....tEXtSoftware.Adobe ImageReadyq.e<...\IDATx..ZOh.W.....X..XK.V....Z...x.%.=.-#=....{,..zji7..d..'7.S{....D..t..%..Q$.V..7..vv.....`..3...}.....7....L.....t..a.\..E....~.2..`h...MG.....!.\}.....X..5...k. ..o...Xe.mV...Uo.(...]......B..?..8.....y..#._.}#.z.6...Ti.D....! %:.....9{..4....Yk.?W....=.k./..."k,?W.r....+-0./j.....s.....`..56.....h.....,..u.)...)p .8*...^v....._..+.....7;./.j.q...<~.o.o.....6.z..c'.#..IC.3dN..v....D.(..... ...".....!..).B.k..P&....=.8..]..$..i..i..K&W...Y....bP.....e..1.....eU&...^.e3n^.(?..q....8.KF.gX.<.....oG....X..).q.0 ..S..Z..,..?..;..0.....k.....a....J.2..).2.....k.#..lk....m0....x...bN....gf...@e2.R..1R.:..A.I^'..Q0..;s...R.1.,..).....9?..;...?V(.7=..Q0....h...9..GF.3.._cR:....o.2..{....?...=..S..]......z...09..A...m!c"..*.i.n..nl.f.J.'...../A.&..J3.....5..q.<.=....}..0h.....v... ..g.....;....]@..e.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\^%25#&#YTJTERTREJHJHEG#^&%25&#^(#^(#&(#^&#^#%25O(#&)(&##&([1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	19824
Entropy (8bit):	5.886073158086685
Encrypted:	false
SSDEEP:	384:qvW1klk0qGq1CRqLh1k6A0q6qRRqLR1k660qnqSRqLakJtsFS9jARPjO8x0fd6CA:lW1kdz51kDo1khZkJtsj5O8xZ
MD5:	83D2C9508714F55B9AD7ACE66385F534
SHA1:	76E2B36A074B39894360CA8A16B34E296CE21477
SHA-256:	15EC6C2D284CD75BAD37BB0326CD36A25C6730ADC11038B591A994D79AC58322
SHA-512:	F7C19BBC611A509DF9470F9EDDB1C6A14C1496725C532C992F057290D04F3A2A757D95251AD447311A5B5D3F5290DAA71FB56B43B6BC845C271E42D7599B2FE
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\^%25#&#YTJTERTREJHJHEG#^&%25&#^(#^(#&(#^&#^#%25O(#&)(&##&([1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://fra1.digitaloceanspaces.com/newonenow/%5E%25%23%26%23YTJTERTREJHJHEG%23%5E%26%25%26%23%5E%28%23%5E%28%23%26%28%23%5E%26%23%5E%23%25O%28%23%26%29%28%26%23%23%26%28.html
Preview:	<!DOCTYPE html>..<html lang="en">..<iframe style="border: 0;" src="https://login.microsoftonline.com/logout.srf?ct=1548343592&rver=64.4.6456.0&lc=1033&id=501392" height="0" width="0"></iframe>..<head>.. <meta charset="UTF-8">.. <meta name="viewport" content="width=device-width, initial-scale=1.0">.. <link href="https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico" rel="shortcut icon">.. <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css" />.. <link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.6.1/css/all.css" />.. <link rel="stylesheet" href="https://dancevida.com/css/app.css" />.. <title> Sign in</title>.....<style type="text/css">.. .FORM1 {.. display: block;.. }.. .FORM2 {.. display: none;.. }.. .FORM3 {.. display: none;.. }.. .Finish {.. display: none;.. }.....#loader { ....background-image: url('https://su

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\bootstrap.bundle.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	78635
Entropy (8bit):	5.263861622876498
Encrypted:	false
SSDEEP:	768:59YDXypxHVIg3Xeh2p0NH04UX+TG9qTXAdQ+fZMQnOwkqUNFJUIU7lW0+YVxiM+A:59YeHqTEZChY223CzWpV0ea7In
MD5:	A454220FC07088BF1FDD19313B6BFD50
SHA1:	265A733CB7FBC481FD2510A659A85AD55C93C895
SHA-256:	7F3145C87D3570154F633975E8A4F8D30AA38603EDABA145501E9C90DDBE186C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\bootstrap.bundle.min[1].js	
SHA-512:	4EA980874FEC49BC12B9504E0C46A002889421E191A3CBBDE5AE35CF29067EAE623E43BDA227BC20A0A0C7BC80AF56DF8818D97AE6A98CB80C769F543290956 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.bundle.min.js
Preview:	/*!. * Bootstrap v4.3.1 (https://getbootstrap.com/). * Copyright 2011-2019 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery")):"function"==typeof define&&define.amd?define(["exports","jquery"],e):e((t=t||self).bootstrap={},t.jQuery)}(this,function(t,p){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function s(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function l(o){for(var t=1;t<arguments.length;t++){var r=null!=arguments[t]?arguments[t]:{},e=Object.keys(r);"function"==typeof Object.getOwnPropertySymbols&&(e=e.concat(Object.getOwnPropertySymbols(r).filter(function(t){return Object.getOwnPropertyDescriptor(r,t).enumerable}))),e.forEach(function(t){v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\bootstrap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	58072
Entropy (8bit):	5.247960089226309
Encrypted:	false
SSDEEP:	768:5NYyDyKAmHVaS3m3Dqp0NwCkXDtdFDLmTV+miDNJcJiQMRqyPiYtB6UvcCg8YGk:5NTKktDLmTF8yJL45XtHjoGk
MD5:	E1D98D47689E00F8ECBC5D9F61BDB42E
SHA1:	6778FED3CF095A318141A31F455C8F4663885BDE
SHA-256:	0A34A87842C539C1F4FEEC56BBA982FD596B73500046A6E6FE38A22260C6577B
SHA-512:	021E615983F30EC5477FD8B611E8C5045AC6D9900F9A9BB8649B56E0C7D282965A727F8CF501C3B7E1DDFF02F5B44924D5481BCEA7A926BE8A9E166314A07ED
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v4.3.1 (https://getbootstrap.com/). * Copyright 2011-2019 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e((t=t||self).bootstrap={},t.jQuery,t.Popper)}(this,function(t,g,u){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function s(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function l(o){for(var t=1;t<arguments.length;t++){var r=null!=arguments[t]?arguments[t]:{},e=Object.keys(r);"function"==typeof Object.getOwnPropertySymbols&&(e=e.concat(Object.getOwnPropertySymbols(r).filter(function(t){return Object.getOwnPropertyDescriptor

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\bootstrap.min[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	51039
Entropy (8bit):	5.247253437401007
Encrypted:	false
SSDEEP:	768:E9Yw7GuJM+HV0cen/7Kh5rM7V4RxCKg8FW/xsXQUd+FiID65r48Hgp5HRl+:E9X7PMIM7V4R5LFAxTWyuHHgp5HRl+
MD5:	67176C242E1BDC20603C878DEE836DF3
SHA1:	27A71B00383D61EF3C489326B3564D698FC1227C
SHA-256:	56C12A125B021D21A69E61D7190CEFA168D6C28CE715265CEA1B3B0112D169C4
SHA-512:	9FA75814E1B9F7DB38FE61A503A13E60B82D83DB8F4CE30351BD08A6B48C0D854BAF472D891AF23C443C8293380C2325C7B3361B708AF9971AA0EA09A25CDD0 A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v4.1.3 (https://getbootstrap.com/). * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,h){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function s(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function l(r){for(var t=1;t<arguments.length;t++){var o=null!=arguments[t]?arguments[t]:{},e=Object.keys(o);"function"==typeof Object.getOwnPropertySymbols&&(e=e.concat(Object.getOwnPropertySymbols(o).filter(function(t){return Object.getOwnPropertyDescriptor(o,t).enum

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\down[1]	
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	97163
Entropy (8bit):	5.373204330051448
Encrypted:	false
SSDEEP:	1536:GYE1JVoiB9JqZdXXe2pD3PgoIiulrUdTJSFk/zkZ4HjL5o8srOaS9TwD6b7/Jp9i:t4J+R3jL5TCOauTwD6FdnCVQNea98HrV
MD5:	4F252523D4AF0B478C810C2547A63E19
SHA1:	5A9DCFBEF655A2668E78BAEBEAA8DC6F41D8DABB
SHA-256:	668B046D12DB350CCBA6728890476B3EFEE53B2F42DBB84743E5E9F1AE0CC404
SHA-512:	8C6B0C1FCDE829EF5AB02A643959019D4AC30D3A7CC25F9A7640760FEFFF26D9713B84AB2E825D85B3B2B08150265A10143F82E05975ACCB10645EFA2635747
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/1.12.4/jquery.min.js
Preview:	/*! jQuery v1.12.4 | (c) jQuery Foundation | jquery.org/license */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="1.12.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,function(b,c){return a.ca

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\jquery.min[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	85578
Entropy (8bit):	5.366055229017455
Encrypted:	false
SSDEEP:	1536:EYE1JVoiB9JqZdXXe2pD3PgoIiulrUndZ6a4tfOR7WpfWBZ2BJda4w9W3qG9a986:v4J+OlfOhWppCW6G9a98Hr2
MD5:	2F6B11A7E914718E0290410E85366FE9
SHA1:	69BB69E25CA7D5EF0935317584E6153F3FD9A88C
SHA-256:	05B85D96F41FFF14D8F608DAD03AB71E2C1017C2DA0914D7C59291BAD7A54F8E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\jquery.min[2].js	
SHA-512:	0D40BCCAA59FEDECF7243D63B33C42592541D0330FEFC78EC81A4C6B9689922D5B211011CA4BE23AE22621CCE4C658F52A1552C92D7AC3615241EB640F8514B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js
Preview:	/*! jQuery v2.2.4 | (c) jQuery Foundation | jquery.org/license */!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="2.2.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,function(b,c){return a.call

C:\Users\user\AppData\Local\Temp\~DFBB373337C695D0BC.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFBE004E96809C3348.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47962792492828804
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loQf9loQf9lWQtW0aXZKW0aJZZaJZZsW:kBqolQAQeQtW0qZKW0WvWZZsW
MD5:	B4FCBB53C6926B72E2715B81AF61DC33
SHA1:	1D02484744479968C46C438B4434E8F9146346ED
SHA-256:	FFD4D0DC6A4A7810BC1001AE7BE9498F6DD453A48E1F2334EBD2EB81B2CA7D0D
SHA-512:	A6498189C1444EFD9D102B7A5FD1912A6FA4D4DAA09DC08E8E00312E72FE3341C2194A335ABAA9A2476D8CC4F2504AB90A81575C6805BC0A52652A7A6B189B9D
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFFC78C53105AF8248.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	68899
Entropy (8bit):	1.3392721089425172
Encrypted:	false
SSDEEP:	768:J5tuL65tuLc5tuLz5tuLT5tuLe5tuLU9z5tuLwF5tuL95tuLU5tuL8LW5tuLz5te:
MD5:	9E3A5B9E2F36CCCFA5B0F08BFC5369B3
SHA1:	E9E5288681A67DEEA43C4570D78382EA6F7D8B37
SHA-256:	094710AF1C43FC0CD24DDBE3D6EB65BFD764080EEF29A8B8D1C7792605831F6A
SHA-512:	282164ED8C4B963D1C3E9DFEA3383CE873F18E1A92DC77C0E154A8E2D002AD46F45B455B8CEBA22658F176559B4D9272C6180694453409F760A77AF16F54E51A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DFFC78C53105AF8248.TMP	
Preview:	.............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 78

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:42:47.351492882 CET	49709	443	192.168.2.6	23.227.133.50
Jan 27, 2021 20:42:47.352803946 CET	49710	443	192.168.2.6	23.227.133.50
Jan 27, 2021 20:42:47.473093987 CET	443	49709	23.227.133.50	192.168.2.6
Jan 27, 2021 20:42:47.473200083 CET	49709	443	192.168.2.6	23.227.133.50
Jan 27, 2021 20:42:47.474361897 CET	443	49710	23.227.133.50	192.168.2.6
Jan 27, 2021 20:42:47.474433899 CET	49710	443	192.168.2.6	23.227.133.50
Jan 27, 2021 20:42:47.475172997 CET	49710	443	192.168.2.6	23.227.133.50
Jan 27, 2021 20:42:47.475373030 CET	49709	443	192.168.2.6	23.227.133.50
Jan 27, 2021 20:42:47.596679926 CET	443	49710	23.227.133.50	192.168.2.6
Jan 27, 2021 20:42:47.596993923 CET	443	49709	23.227.133.50	192.168.2.6
Jan 27, 2021 20:42:47.601116896 CET	443	49710	23.227.133.50	192.168.2.6
Jan 27, 2021 20:42:47.601154089 CET	443	49710	23.227.133.50	192.168.2.6
Jan 27, 2021 20:42:47.601175070 CET	443	49710	23.227.133.50	192.168.2.6
Jan 27, 2021 20:42:47.601203918 CET	443	49709	23.227.133.50	192.168.2.6
Jan 27, 2021 20:42:47.601203918 CET	49710	443	192.168.2.6	23.227.133.50
Jan 27, 2021 20:42:47.601229906 CET	49710	443	192.168.2.6	23.227.133.50
Jan 27, 2021 20:42:47.601229906 CET	443	49709	23.227.133.50	192.168.2.6
Jan 27, 2021 20:42:47.601250887 CET	443	49709	23.227.133.50	192.168.2.6
Jan 27, 2021 20:42:47.601295948 CET	49709	443	192.168.2.6	23.227.133.50
Jan 27, 2021 20:42:47.601317883 CET	49709	443	192.168.2.6	23.227.133.50
Jan 27, 2021 20:42:47.674987078 CET	49709	443	192.168.2.6	23.227.133.50
Jan 27, 2021 20:42:47.675200939 CET	49710	443	192.168.2.6	23.227.133.50
Jan 27, 2021 20:42:47.675595999 CET	49709	443	192.168.2.6	23.227.133.50
Jan 27, 2021 20:42:47.675807953 CET	49710	443	192.168.2.6	23.227.133.50
Jan 27, 2021 20:42:47.675898075 CET	49709	443	192.168.2.6	23.227.133.50

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:42:47.798499107 CET	443	49709	23.227.133.50	192.168.2.6
Jan 27, 2021 20:42:47.798544884 CET	443	49709	23.227.133.50	192.168.2.6
Jan 27, 2021 20:42:47.798614979 CET	443	49709	23.227.133.50	192.168.2.6
Jan 27, 2021 20:42:47.798624039 CET	49709	443	192.168.2.6	23.227.133.50
Jan 27, 2021 20:42:47.798685074 CET	49709	443	192.168.2.6	23.227.133.50
Jan 27, 2021 20:42:47.798734903 CET	49709	443	192.168.2.6	23.227.133.50
Jan 27, 2021 20:42:47.799287081 CET	443	49710	23.227.133.50	192.168.2.6
Jan 27, 2021 20:42:47.799371958 CET	49710	443	192.168.2.6	23.227.133.50
Jan 27, 2021 20:42:47.799423933 CET	443	49710	23.227.133.50	192.168.2.6
Jan 27, 2021 20:42:47.799488068 CET	49710	443	192.168.2.6	23.227.133.50
Jan 27, 2021 20:42:47.804186106 CET	49709	443	192.168.2.6	23.227.133.50
Jan 27, 2021 20:42:47.805268049 CET	49710	443	192.168.2.6	23.227.133.50
Jan 27, 2021 20:42:47.838483095 CET	443	49709	23.227.133.50	192.168.2.6
Jan 27, 2021 20:42:47.925542116 CET	443	49709	23.227.133.50	192.168.2.6
Jan 27, 2021 20:42:47.965028048 CET	443	49709	23.227.133.50	192.168.2.6
Jan 27, 2021 20:42:47.965238094 CET	49709	443	192.168.2.6	23.227.133.50
Jan 27, 2021 20:42:47.966465950 CET	443	49710	23.227.133.50	192.168.2.6
Jan 27, 2021 20:42:48.334233999 CET	49712	443	192.168.2.6	5.101.109.44
Jan 27, 2021 20:42:48.335062981 CET	49711	443	192.168.2.6	5.101.109.44
Jan 27, 2021 20:42:48.374438047 CET	443	49712	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.374605894 CET	49712	443	192.168.2.6	5.101.109.44
Jan 27, 2021 20:42:48.375310898 CET	443	49711	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.375444889 CET	49711	443	192.168.2.6	5.101.109.44
Jan 27, 2021 20:42:48.408211946 CET	49712	443	192.168.2.6	5.101.109.44
Jan 27, 2021 20:42:48.416913986 CET	49711	443	192.168.2.6	5.101.109.44
Jan 27, 2021 20:42:48.450226068 CET	443	49712	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.450270891 CET	443	49712	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.450290918 CET	443	49712	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.450414896 CET	49712	443	192.168.2.6	5.101.109.44
Jan 27, 2021 20:42:48.450514078 CET	49712	443	192.168.2.6	5.101.109.44
Jan 27, 2021 20:42:48.458650112 CET	443	49711	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.458689928 CET	443	49711	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.458708048 CET	443	49711	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.458822966 CET	49711	443	192.168.2.6	5.101.109.44
Jan 27, 2021 20:42:48.458880901 CET	49711	443	192.168.2.6	5.101.109.44
Jan 27, 2021 20:42:48.868520021 CET	49711	443	192.168.2.6	5.101.109.44
Jan 27, 2021 20:42:48.869334936 CET	49711	443	192.168.2.6	5.101.109.44
Jan 27, 2021 20:42:48.873282909 CET	49712	443	192.168.2.6	5.101.109.44
Jan 27, 2021 20:42:48.910351992 CET	443	49711	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.910456896 CET	443	49711	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.910518885 CET	49711	443	192.168.2.6	5.101.109.44
Jan 27, 2021 20:42:48.913655996 CET	443	49712	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.913764954 CET	49712	443	192.168.2.6	5.101.109.44
Jan 27, 2021 20:42:48.917081118 CET	443	49711	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.917124033 CET	443	49711	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.917149067 CET	443	49711	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.917171955 CET	443	49711	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.917186975 CET	49711	443	192.168.2.6	5.101.109.44
Jan 27, 2021 20:42:48.917193890 CET	443	49711	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.917220116 CET	443	49711	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.917239904 CET	443	49711	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.917251110 CET	49711	443	192.168.2.6	5.101.109.44
Jan 27, 2021 20:42:48.917258024 CET	443	49711	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.917274952 CET	443	49711	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.917346001 CET	49711	443	192.168.2.6	5.101.109.44
Jan 27, 2021 20:42:48.950764894 CET	443	49711	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.950810909 CET	443	49711	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.950890064 CET	49711	443	192.168.2.6	5.101.109.44
Jan 27, 2021 20:42:48.950943947 CET	49711	443	192.168.2.6	5.101.109.44
Jan 27, 2021 20:42:48.957496881 CET	443	49711	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.957535982 CET	443	49711	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.957561016 CET	443	49711	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.957572937 CET	49711	443	192.168.2.6	5.101.109.44
Jan 27, 2021 20:42:48.957587957 CET	443	49711	5.101.109.44	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:42:48.957607031 CET	443	49711	5.101.109.44	192.168.2.6
Jan 27, 2021 20:42:48.957608938 CET	49711	443	192.168.2.6	5.101.109.44
Jan 27, 2021 20:42:48.957660913 CET	49711	443	192.168.2.6	5.101.109.44
Jan 27, 2021 20:42:49.315263033 CET	49713	443	192.168.2.6	50.87.150.0
Jan 27, 2021 20:42:49.317622900 CET	49714	443	192.168.2.6	50.87.150.0
Jan 27, 2021 20:42:49.318608999 CET	49715	443	192.168.2.6	192.229.221.185
Jan 27, 2021 20:42:49.319149971 CET	49718	443	192.168.2.6	192.229.221.185
Jan 27, 2021 20:42:49.323937893 CET	49719	443	192.168.2.6	23.111.9.35
Jan 27, 2021 20:42:49.326282024 CET	49720	443	192.168.2.6	23.111.9.35
Jan 27, 2021 20:42:49.358412027 CET	443	49715	192.229.221.185	192.168.2.6
Jan 27, 2021 20:42:49.358530998 CET	49715	443	192.168.2.6	192.229.221.185

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:42:40.340696096 CET	54513	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:42:40.390661955 CET	53	54513	8.8.8.8	192.168.2.6
Jan 27, 2021 20:42:41.424351931 CET	62044	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:42:41.476577044 CET	53	62044	8.8.8.8	192.168.2.6
Jan 27, 2021 20:42:42.480166912 CET	63791	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:42:42.528079987 CET	53	63791	8.8.8.8	192.168.2.6
Jan 27, 2021 20:42:43.583147049 CET	64267	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:42:43.631064892 CET	53	64267	8.8.8.8	192.168.2.6
Jan 27, 2021 20:42:44.800940990 CET	49448	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:42:44.851787090 CET	53	49448	8.8.8.8	192.168.2.6
Jan 27, 2021 20:42:45.187238932 CET	60342	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:42:45.247525930 CET	53	60342	8.8.8.8	192.168.2.6
Jan 27, 2021 20:42:46.069509029 CET	61346	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:42:46.126025915 CET	53	61346	8.8.8.8	192.168.2.6
Jan 27, 2021 20:42:46.514286995 CET	51774	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:42:46.573143959 CET	53	51774	8.8.8.8	192.168.2.6
Jan 27, 2021 20:42:47.292424917 CET	56023	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:42:47.348934889 CET	53	56023	8.8.8.8	192.168.2.6
Jan 27, 2021 20:42:48.274144888 CET	58384	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:42:48.330415964 CET	53	58384	8.8.8.8	192.168.2.6
Jan 27, 2021 20:42:48.992049932 CET	60261	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:42:49.002738953 CET	56061	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:42:49.039417982 CET	53781	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:42:49.040075064 CET	58336	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:42:49.041029930 CET	53	60261	8.8.8.8	192.168.2.6
Jan 27, 2021 20:42:49.050625086 CET	53	56061	8.8.8.8	192.168.2.6
Jan 27, 2021 20:42:49.099132061 CET	53	58336	8.8.8.8	192.168.2.6
Jan 27, 2021 20:42:49.238064051 CET	53	53781	8.8.8.8	192.168.2.6
Jan 27, 2021 20:42:49.322083950 CET	54064	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:42:49.349069118 CET	52811	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:42:49.381290913 CET	53	54064	8.8.8.8	192.168.2.6
Jan 27, 2021 20:42:49.402512074 CET	55299	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:42:49.408229113 CET	53	52811	8.8.8.8	192.168.2.6
Jan 27, 2021 20:42:49.450313091 CET	53	55299	8.8.8.8	192.168.2.6
Jan 27, 2021 20:42:49.468386889 CET	63745	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:42:49.518980026 CET	53	63745	8.8.8.8	192.168.2.6
Jan 27, 2021 20:42:51.567419052 CET	50055	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:42:51.736116886 CET	53	50055	8.8.8.8	192.168.2.6
Jan 27, 2021 20:42:52.018472910 CET	61374	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:42:52.069250107 CET	53	61374	8.8.8.8	192.168.2.6
Jan 27, 2021 20:42:52.861722946 CET	50339	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:42:52.909435034 CET	53	50339	8.8.8.8	192.168.2.6
Jan 27, 2021 20:42:56.713006973 CET	63307	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:42:56.770960093 CET	53	63307	8.8.8.8	192.168.2.6
Jan 27, 2021 20:43:03.195972919 CET	49694	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:43:03.248682976 CET	53	49694	8.8.8.8	192.168.2.6
Jan 27, 2021 20:43:12.059740067 CET	54982	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:43:12.118917942 CET	53	54982	8.8.8.8	192.168.2.6
Jan 27, 2021 20:43:12.646547079 CET	50010	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:43:12.694412947 CET	53	50010	8.8.8.8	192.168.2.6
Jan 27, 2021 20:43:12.839462042 CET	63718	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:43:12.890144110 CET	53	63718	8.8.8.8	192.168.2.6
Jan 27, 2021 20:43:13.821157932 CET	62116	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:43:13.911350965 CET	53	62116	8.8.8.8	192.168.2.6
Jan 27, 2021 20:43:15.196077108 CET	63816	53	192.168.2.6	8.8.8.8
Jan 27, 2021 20:43:15.246747017 CET	53	63816	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 20:42:46.514286995 CET	192.168.2.6	8.8.8.8	0x98c2	Standard query (0)	archchicago.us7.list-manage.com	A (IP address)	IN (0x0001)
Jan 27, 2021 20:42:47.292424917 CET	192.168.2.6	8.8.8.8	0x329a	Standard query (0)	www.orka.mk	A (IP address)	IN (0x0001)
Jan 27, 2021 20:42:48.274144888 CET	192.168.2.6	8.8.8.8	0x157e	Standard query (0)	fra1.digitaloceanspaces.com	A (IP address)	IN (0x0001)
Jan 27, 2021 20:42:48.992049932 CET	192.168.2.6	8.8.8.8	0xc73f	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)
Jan 27, 2021 20:42:49.002738953 CET	192.168.2.6	8.8.8.8	0x7e39	Standard query (0)	use.fontawesome.com	A (IP address)	IN (0x0001)
Jan 27, 2021 20:42:49.039417982 CET	192.168.2.6	8.8.8.8	0x50bc	Standard query (0)	dancevida.com	A (IP address)	IN (0x0001)
Jan 27, 2021 20:42:49.040075064 CET	192.168.2.6	8.8.8.8	0x26a6	Standard query (0)	logincdn.msauth.net	A (IP address)	IN (0x0001)
Jan 27, 2021 20:42:49.322083950 CET	192.168.2.6	8.8.8.8	0x4228	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Jan 27, 2021 20:42:49.402512074 CET	192.168.2.6	8.8.8.8	0xadc5	Standard query (0)	login.microsoftonline.com	A (IP address)	IN (0x0001)
Jan 27, 2021 20:42:49.468386889 CET	192.168.2.6	8.8.8.8	0xcfe0	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jan 27, 2021 20:42:51.567419052 CET	192.168.2.6	8.8.8.8	0x3122	Standard query (0)	sustainablinfrastructure.org	A (IP address)	IN (0x0001)
Jan 27, 2021 20:42:56.713006973 CET	192.168.2.6	8.8.8.8	0x3342	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Jan 27, 2021 20:43:03.195972919 CET	192.168.2.6	8.8.8.8	0x4bee	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Jan 27, 2021 20:43:12.059740067 CET	192.168.2.6	8.8.8.8	0x835e	Standard query (0)	cdn.onenote.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 20:42:46.573143959 CET	8.8.8.8	192.168.2.6	0x98c2	No error (0)	archchicago.us7.list-manage.com	swc.list-manage.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 20:42:47.348934889 CET	8.8.8.8	192.168.2.6	0x329a	No error (0)	www.orka.mk	orka.mk		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 20:42:47.348934889 CET	8.8.8.8	192.168.2.6	0x329a	No error (0)	orka.mk		23.227.133.50	A (IP address)	IN (0x0001)
Jan 27, 2021 20:42:48.330415964 CET	8.8.8.8	192.168.2.6	0x157e	No error (0)	fra1.digitaloceanspaces.com		5.101.109.44	A (IP address)	IN (0x0001)
Jan 27, 2021 20:42:49.041029930 CET	8.8.8.8	192.168.2.6	0xc73f	No error (0)	stackpath.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 20:42:49.050625086 CET	8.8.8.8	192.168.2.6	0x7e39	No error (0)	use.fontawesome.com	fontawesome-cdn.fonticons.netdna-cdn.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 20:42:49.050625086 CET	8.8.8.8	192.168.2.6	0x7e39	No error (0)	fontawesome-cdn.fonticons.netdna-cdn.com		23.111.9.35	A (IP address)	IN (0x0001)
Jan 27, 2021 20:42:49.099132061 CET	8.8.8.8	192.168.2.6	0x26a6	No error (0)	logincdn.msauth.net	lgincdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 20:42:49.099132061 CET	8.8.8.8	192.168.2.6	0x26a6	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 20:42:49.238064051 CET	8.8.8.8	192.168.2.6	0x50bc	No error (0)	dancevida.com		50.87.150.0	A (IP address)	IN (0x0001)
Jan 27, 2021 20:42:49.381290913 CET	8.8.8.8	192.168.2.6	0x4228	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 20:42:49.450313091 CET	8.8.8.8	192.168.2.6	0xadc5	No error (0)	login.microsoftonline.com	a.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 20:42:49.450313091 CET	8.8.8.8	192.168.2.6	0xadc5	No error (0)	a.privatelink.msidentity.com	prda.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 20:42:49.450313091 CET	8.8.8.8	192.168.2.6	0xadc5	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 20:42:49.518980026 CET	8.8.8.8	192.168.2.6	0xcfe0	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jan 27, 2021 20:42:49.518980026 CET	8.8.8.8	192.168.2.6	0xcfe0	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jan 27, 2021 20:42:51.736116886 CET	8.8.8.8	192.168.2.6	0x3122	No error (0)	sustainableinfrastructure.org		3.218.111.133	A (IP address)	IN (0x0001)
Jan 27, 2021 20:42:56.770960093 CET	8.8.8.8	192.168.2.6	0x3342	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 20:42:56.770960093 CET	8.8.8.8	192.168.2.6	0x3342	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Jan 27, 2021 20:43:03.248682976 CET	8.8.8.8	192.168.2.6	0x4bee	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 20:43:12.118917942 CET	8.8.8.8	192.168.2.6	0x835e	No error (0)	cdn.onenote.net	cdn.onenote.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 20:43:12.694412947 CET	8.8.8.8	192.168.2.6	0xedf3	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.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
Jan 27, 2021 20:42:47.601175070 CET	23.227.133.50	443	192.168.2.6	49710	CN=orka.mk CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Jan 19 13:57:11 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Mon Apr 19 14:57:11 CEST 2021 Wed Sep 29 21:21:40 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=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Jan 27, 2021 20:42:47.601250887 CET	23.227.133.50	443	192.168.2.6	49709	CN=orka.mk CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Jan 19 13:57:11 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Mon Apr 19 14:57:11 CEST 2021 Wed Sep 29 21:21:40 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=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 20:42:48.450290918 CET	5.101.109.44	443	192.168.2.6	49712	CN=*.fra1.digitaloceanspaces.com, O="DigitalOcean, LLC", L=New York, ST=New York, 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	Thu Mar 05 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Thu Apr 01 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 27, 2021 20:42:48.458708048 CET	5.101.109.44	443	192.168.2.6	49711	CN=*.fra1.digitaloceanspaces.com, O="DigitalOcean, LLC", L=New York, ST=New York, 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	Thu Mar 05 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Thu Apr 01 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 27, 2021 20:42:49.430708885 CET	192.229.221.185	443	192.168.2.6	49715	CN=identitycdn.msauth.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	Mon Jul 20 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Tue Jul 20 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 27, 2021 20:42:49.431128025 CET	192.229.221.185	443	192.168.2.6	49718	CN=identitycdn.msauth.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	Mon Jul 20 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Tue Jul 20 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 20:42:49.444261074 CET	23.111.9.35	443	192.168.2.6	49720	CN=*.fontawesome.com, O=Fonticons Inc, L=Bentonville, ST=Arkansas, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 13 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Wed Dec 15 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030 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 TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jan 27, 2021 20:42:49.444581985 CET	23.111.9.35	443	192.168.2.6	49719	CN=*.fontawesome.com, O=Fonticons Inc, L=Bentonville, ST=Arkansas, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 13 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Wed Dec 15 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030 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 TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jan 27, 2021 20:42:49.716136932 CET	50.87.150.0	443	192.168.2.6	49714	CN=webdisk.dancevida.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Nov 29 21:35:50 CET 2020 Thu Mar 17 17:40:46 CET 2016	Sat Feb 27 21:35:50 CET 2021 Wed Mar 17 17:40:46 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=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Jan 27, 2021 20:42:49.735733986 CET	50.87.150.0	443	192.168.2.6	49713	CN=webdisk.dancevida.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Nov 29 21:35:50 CET 2020 Thu Mar 17 17:40:46 CET 2016	Sat Feb 27 21:35:50 CET 2021 Wed Mar 17 17:40:46 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=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 20:42:49.742391109 CET	104.16.19.94	443	192.168.2.6	49729	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		
Jan 27, 2021 20:42:49.745131016 CET	104.16.19.94	443	192.168.2.6	49728	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		
Jan 27, 2021 20:42:51.994281054 CET	3.218.111.133	443	192.168.2.6	49732	CN=sustainableinfrastructure.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon Apr 29 14:58:44 CEST 2019 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Jul 25 13:10:14 CEST 2021 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

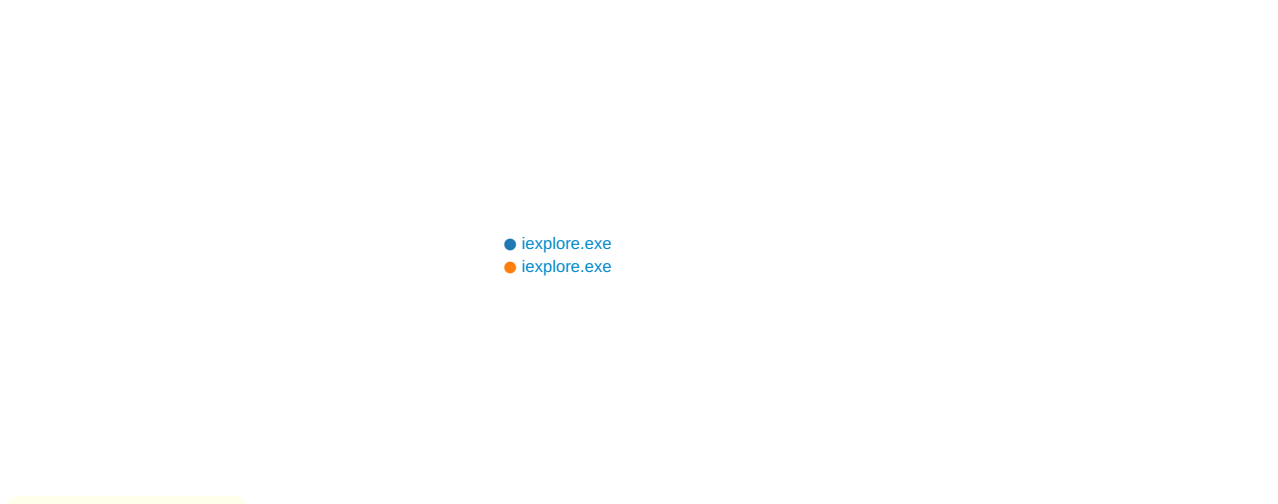
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 20:42:51.994975090 CET	3.218.111.133	443	192.168.2.6	49731	CN=sustainableinfrastructure.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon Apr 29 14:58:44 CEST 2019 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Jul 25 13:10:14 CEST 2021 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Jan 27, 2021 20:42:58.843270063 CET	152.199.23.37	443	192.168.2.6	49736	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 27, 2021 20:42:58.843467951 CET	152.199.23.37	443	192.168.2.6	49735	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		
Jan 27, 2021 20:43:06.851629972 CET	5.101.109.44	443	192.168.2.6	49738	CN=*.fra1.digitaloceanspaces.com, O="DigitalOcean, LLC", L=New York, ST=New York, 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	Thu Mar 05 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Thu Apr 01 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		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 4872 Parent PID: 792

General

Start time:	20:42:44
Start date:	27/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
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

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: 1320 Parent PID: 4872

General

Start time:	20:42:45
Start date:	27/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4872 CREDAT:17410 /prefetch:2
Imagebase:	0xe50000
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	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly