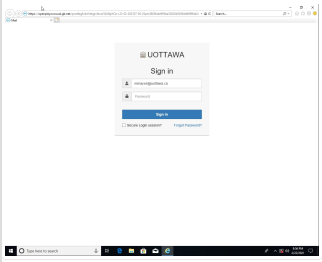
ID: 356287
Cookbook: browseurl.jbs
Time: 20:55:37
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

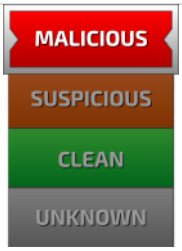
Analysis Report https://architectchintanvirani.com/1/2su…

Overview

General Information

Sample URL:	http://https://architectchintanvirani.com/1/2support/index.php?email=mmaye4@uottawa.ca
Analysis ID:	356287
Most interesting Screenshot:	

Detection



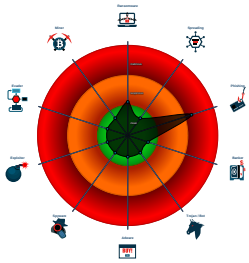
HTMLPhisher

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for doma…
- Yara detected HtmlPhish_10
- HTML body contains low number of …
- No HTML title found
- URL contains potential PII (phishing…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 2024 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 752 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2024 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

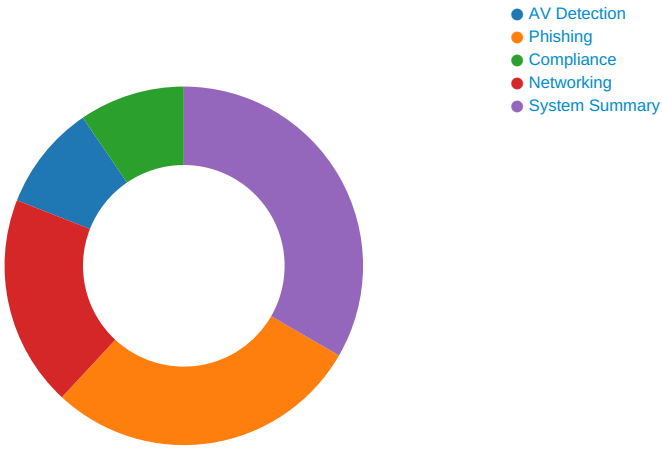
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5309dd609ff4d2cc7b4d82702293091209e3ad38ed14aNHZVVml0czVCRkxRWmswVUVzPQ==UGFraXN0YW4=VUVzPQ==4vUVits5BFLQZk0[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for domain / URL

Phishing:

Yara detected HtmlPhish_10

Compliance:

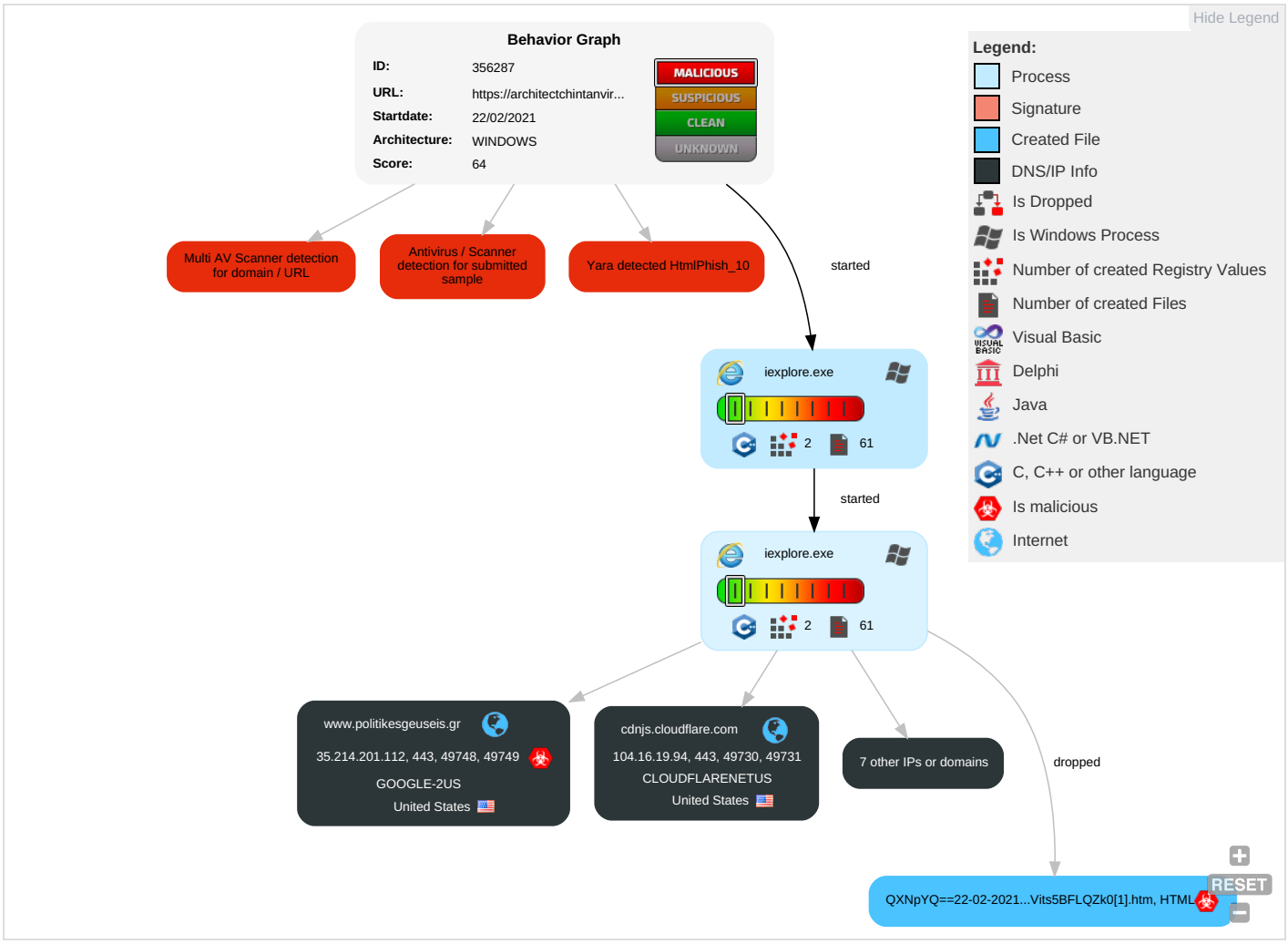
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Mitre Att&ck Matrix

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

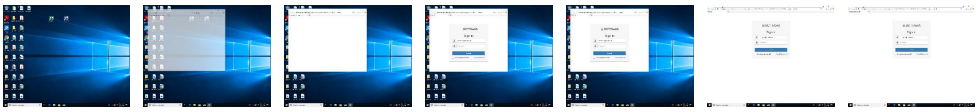
Behavior Graph

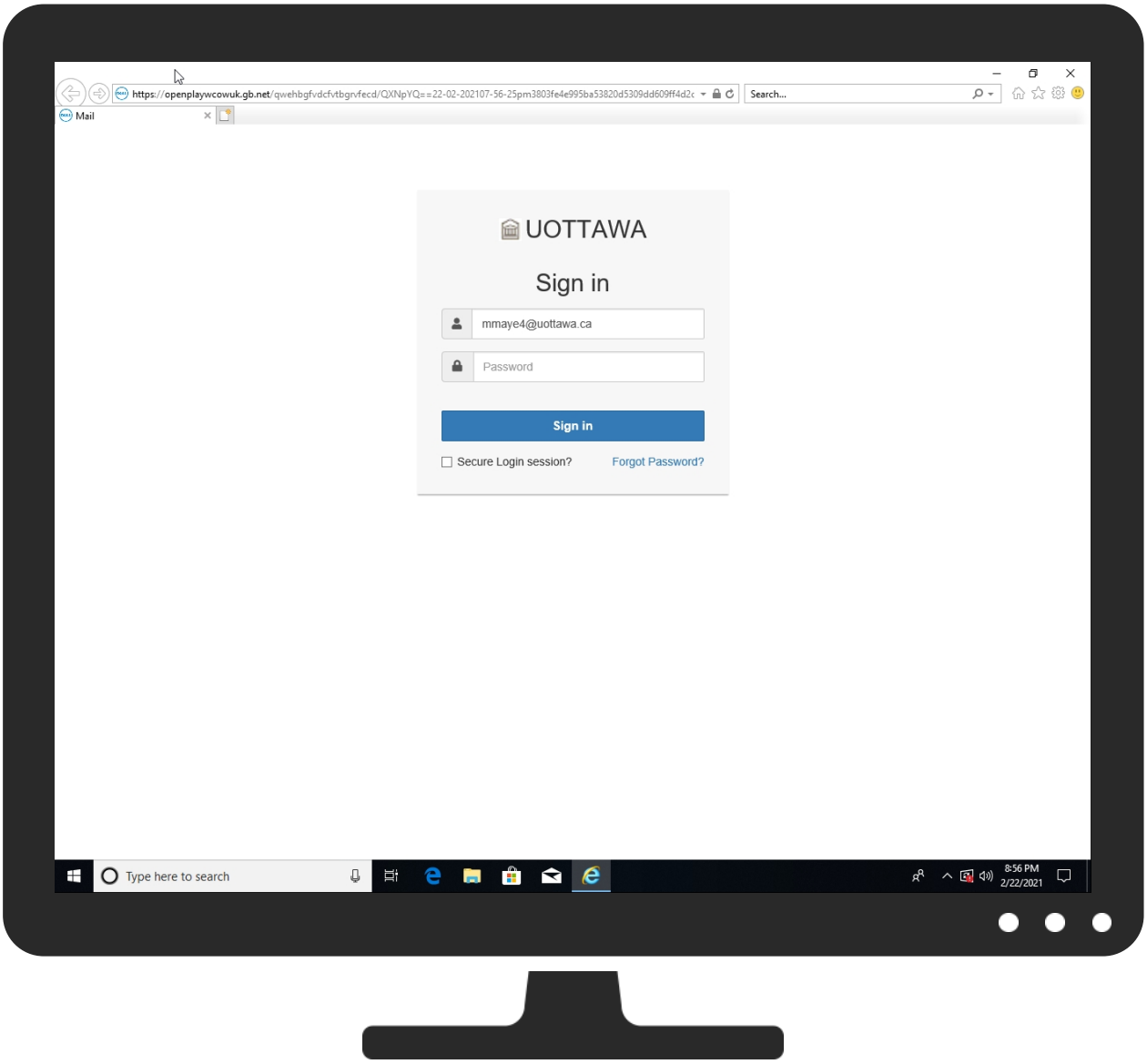


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://architectchintanvirani.com/1/2support/index.php?email=mmaye4@uottawa.ca	0%	Avira URL Cloud	safe	
http://https://architectchintanvirani.com/1/2support/index.php?email=mmaye4@uottawa.ca	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
www.politikesgeuseis.gr	8%	Virustotal		Browse
architectchintanvirani.com	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://openplaywcowuk.gb.net/qwehbgfvdcfvtbgrvfecd/?sicmalsnj3f3=83djnskjac4fr#mmaye4	0%	Avira URL Cloud	safe	
http://https://openplaywcowukanvirani.com/1/2support/index.php?email=mmaye4	0%	Avira URL Cloud	safe	
http://https://openplaywcowuk.gb.net/qwehbgfvdcfvtbgrvfecd/QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5	0%	Avira URL Cloud	safe	
http://https://www.politikesg.gb.net/qwehbgfvdcfvtbgrvfecd/QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5	0%	Avira URL Cloud	safe	
http://https://fontawesome.comhttps://fontawesome.comFont	0%	Avira URL Cloud	safe	
http://https://www.politikesgeuseis.gr/cricl/oauth/site/service/demp.php?email=info	0%	Avira URL Cloud	safe	
http://https://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://openplaywcowuk.gb.net/qwehbgfvdcfvtbgrvfecd/?sicmalsnj3f3=83djnskjac4fr	0%	Avira URL Cloud	safe	
http://https://melissadatawde.ru/ghyjunhtbgvsadrbt18feb/next.php	0%	Avira URL Cloud	safe	
http://https://architectchintanvirani.com/1/2support/index.php?email=mmaye4	0%	Avira URL Cloud	safe	
http://getbootstrap.com)	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
openplaywcowuk.gb.net	104.129.25.9	true	false		unknown
www.politikesgeuseis.gr	35.214.201.112	true	true	• 8%, Virustotal, Browse	unknown
cdnjs.cloudflare.com	104.16.19.94	true	false		high
architectchintanvirani.com	173.237.190.111	true	false	• 3%, Virustotal, Browse	unknown
stackpath.bootstrapcdn.com	unknown	unknown	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
maxcdn.bootstrapcdn.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://openplaywcowuk.gb.net/qwehbgfvdcfvtbgrvfecd/QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5309dd609ff4d2cc7b4d82702293091209e3ad38ed14aNHZVVml0czVCRkxRWmswVUVzPQ==UGFraXN0YW4=VUVzPQ==4vUVits5BFLQZk0/?Key=QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5309dd609ff4d2cc7b4d82702293091209e3ad38ed14aNHZVVml0czVCRkxRWmswVUVzPQ==UGFraXN0YW4=VUVzPQ==4vUVits5BFLQZk0&rand=13InboxLightaspxn_QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5309dd609ff4d2cc7b4d82702293091209e3ad38ed14aNHZVVml0czVCRkxRWmswVUVzPQ==UGFraXN0YW4=VUVzPQ==4vUVits5BFLQZk0_NHZVVml0czVCRkxRWmsw-&21613cde29049b3c91b62de76cfc8570a2e0ec37b8668ec5d246bab8a58db410#mmaye4@uottawa.ca	true		unknown
http://https://www.politikesgeuseis.gr/cricl/oauth/site/service/demp.php?email=info@dell.com#	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://openplaywcowuk.gb.net/qwehbgfvdcfvtbgrvfecd/?sicmalsnj3f3=83djnskjac4fr#mmaye4	~DF5C6855DB7C39EC1D.TMP.1.dr, {78E9B5C8-7593-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://fontawesome.io	font-awesome.min[1].css.3.dr	false		high
http://https://openplaywcowukanvirani.com/1/2support/index.php?email=mmaye4	{78E9B5C8-7593-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://ka-f.fontawesome.com	585b051251[1].js.3.dr	false		high
http://https://code.jquery.com/jquery-3.2.1.slim.min.js	QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5309dd609ff4d2cc7b4d82702293091209e3ad38ed14aNHZVVml0czVCRkxRWmswVUVzPQ==UGFraXN0YW4=VUVzPQ==4vUVits5BFLQZk0[1].htm0.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://code.jquery.com/jquery-3.1.1.min.js	QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5309dd609ff4d2cc7b4d82702293091209e3ad38ed14aNHZVVml0czVCRkxRWmswVUVzPQ==UGFraXN0YW4=VUVzPQ==4vUVits5BFLQZk0[1].htm0.3.dr	false		high
http://https://openplaywcowuk.gb.net/qwehbgfvdcfvtbgrvfecd/QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5	~DF5C6855DB7C39EC1D.TMP.1.dr, QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5309dd609ff4d2cc7b4d82702293091209e3ad38ed14aNHZVVml0czVCRkxRWmswVUVzPQ==UGFraXN0YW4=VUVzPQ==4vUVits5BFLQZk0[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js	QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5309dd609ff4d2cc7b4d82702293091209e3ad38ed14aNHZVVml0czVCRkxRWmswVUVzPQ==UGFraXN0YW4=VUVzPQ==4vUVits5BFLQZk0[1].htm0.3.dr	false		high
http://https://getbootstrap.com/)	bootstrap.min[1].js.3.dr	false		high
http://https://www.politikesg.gb.net/qwehbgfvdcfvtbgrvfecd/QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5	{78E9B5C8-7593-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://fontawesome.comhttps://fontawesome.comFont	free-fa-regular-400[1].eot.3.dr, free-fa-solid-900[1].eot.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://code.jquery.com/jquery-3.3.1.js	QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5309dd609ff4d2cc7b4d82702293091209e3ad38ed14aNHZVVml0czVCRkxRWmswVUVzPQ==UGFraXN0YW4=VUVzPQ==4vUVits5BFLQZk0[1].htm0.3.dr	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css	QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5309dd609ff4d2cc7b4d82702293091209e3ad38ed14aNHZVVml0czVCRkxRWmswVUVzPQ==UGFraXN0YW4=VUVzPQ==4vUVits5BFLQZk0[1].htm0.3.dr	false		high
http://https://fontawesome.com/license/free	free.min[1].css.3.dr	false		high
http://fontawesome.io/license	font-awesome.min[1].css.3.dr	false		high
http://https://fontawesome.com	free-fa-regular-400[1].eot.3.dr, free.min[1].css.3.dr	false		high
http://https://kit.fontawesome.com	585b051251[1].js.3.dr	false		high
http://https://www.politikesgeuseis.gr/cricl/oauth/site/service/demp.php?email=info	QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5309dd609ff4d2cc7b4d82702293091209e3ad38ed14aNHZVVml0czVCRkxRWmswVUVzPQ==UGFraXN0YW4=VUVzPQ==4vUVits5BFLQZk0[1].htm0.3.dr	true	• Avira URL Cloud: safe	unknown
http://https://github.com/twbs/bootstrap/graphs/contributors)	bootstrap.min[2].js.3.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js	QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5309dd609ff4d2cc7b4d82702293091209e3ad38ed14aNHZVVml0czVCRkxRWmswVUVzPQ==UGFraXN0YW4=VUVzPQ==4vUVits5BFLQZk0[1].htm0.3.dr	false		high
http://https://getbootstrap.com)	bootstrap.min[2].js.3.dr	false	• Avira URL Cloud: safe	low
http://https://openplaywcowuk.gb.net/qwehbgfvdcfvtbgrvfecd/?sicmalsnj3f3=83djnskjac4fr	~DF5C6855DB7C39EC1D.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://melissadatawde.ru/ghyjunhtbgvsadrbt18feb/next.php	QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5309dd609ff4d2cc7b4d82702293091209e3ad38ed14aNHZVVml0czVCRkxRWmswVUVzPQ==UGFraXN0YW4=VUVzPQ==4vUVits5BFLQZk0[1].htm0.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://architectchintanvirani.com/1/2support/index.php?email=mmaye4	~DF5C6855DB7C39EC1D.TMP.1.dr, {78E9B5C8-7593-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://getbootstrap.com)	bootstrap.min[1].css.3.dr	false	• Avira URL Cloud: safe	low
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[2].js.3.dr, bootstrap.min[1].css.3.dr	false		high
http://opensource.org/licenses/MIT).	popper.min[1].js.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://kit.fontawesome.com/585b051251.js	QXNpYQ==22-02-202107-56-25pm38 03fe4e995ba53820d5309dd609ff4d 2cc7b4d82702293091209e3ad38ed1 4aNHZVVml0czVCRkxRWm swVUVzPQ==UGFraXN0YW 4=VUVzPQ==4vUVits5BFLQZk0[1].h tm0.3.dr	false		high
http:// https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js	QXNpYQ==22-02-202107-56-25pm38 03fe4e995ba53820d5309dd609ff4d 2cc7b4d82702293091209e3ad38ed1 4aNHZVVml0czVCRkxRWm swVUVzPQ==UGFraXN0YW 4=VUVzPQ==4vUVits5BFLQZk0[1].h tm0.3.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
173.237.190.111	unknown	United States		30496	AS-TIERP-30496US	false
35.214.201.112	unknown	United States		19527	GOOGLE-2US	true
104.129.25.9	unknown	United States		8100	ASN-QUADRANET-GLOBALUS	false
104.16.19.94	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356287
Start date:	22.02.2021
Start time:	20:55:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 49s
Hypervisor based Inspection enabled:	false
Report type:	light

Cookbook file name:	browseurl.jbs
Sample URL:	http://https://architectchintanvirani.com/1/2support/index.php?email=mmaye4@uottawa.ca
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:	7
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:	mal64.phis.win@3/31@9/4
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://www.politikesgeuseis.gr/cricl/oauth/site/service/demp.php?email=info@dell.com#
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): 40.88.32.150, 52.147.198.201, 104.108.39.131, 209.197.3.24, 142.250.185.106, 104.18.22.52, 104.18.23.52, 142.250.185.234, 216.58.212.170, 209.197.3.15, 172.64.203.28, 172.64.202.28, 142.250.185.164, 142.250.186.131, 51.11.168.160, 152.199.19.161, 23.210.248.85 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, cds.s5x3j6q5.hwcdn.net, arc.msn.com.nsatc.net, ka-f.fontawesome.com.cdn.cloudflare.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, www.google.com, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, firebasestorage.googleapis.com, kit.fontawesome.com.cdn.cloudflare.net, fonts.googleapis.com, fs.microsoft.com, ajax.googleapis.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, e1723.g.akamaiedge.net, skypedataprdcoleus16.cloudapp.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cds.j3z9t3p6.hwcdn.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{78E9B5C6-7593-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8564109831188322
Encrypted:	false
SSDEEP:	96:rRZOZ/m2/ZW/tnt/tFf/t/xM/tR/t2/tmgf/tmoVsX:rRZOZ+2BWht/fVxMrg4gf4oVsX
MD5:	8F6CA62CE8772F69354490591084F348
SHA1:	9030BC045F0F2BCE4723818F5F1B3C02BA3119A0
SHA-256:	B2B1542E8A935439398DA8D66DD8FF699E6D271F90025F25CB2B901543F8EF15
SHA-512:	9E2046BCBFF837DCF6E0696A45C2527896F4B913ECB518A902446A7A3CFC3F8C62A6AF3905D5409F06A90FF7BB02739D5C3EB50BD943AEA978759C92413B949
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\{78E9B5C8-7593-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	58760
Entropy (8bit):	2.8580188881414923
Encrypted:	false
SSDEEP:	192:r+ZRQx6rkbjt2NWfMHvbwQshRqXT3jVgkvVgEqVoi9VgW:rKmMwHkkUPbtsr+Tzvah
MD5:	1AAF87BA325F243D361070D8DA44039D
SHA1:	709BE2F2CCD953D35E38215E97BE9CA51CF3C85A
SHA-256:	91A55010CA3B1B0F4B9DE6A7562C13F40C4F24003F640F4C9B44D01054C4EEE2
SHA-512:	E77EFB528A8CE6CFF4401757E7BAC653031BF7DC3F87997B0EEB59F636488D5C8A73BE6C7475DDC0CFA2B955D16F55EF68156E69A89A6991B7E91511EB0564F7
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\{7F62BA04-7593-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7F62BA04-7593-11EB-90E4-ECF4BB862DED}.dat	
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5651711827186239
Encrypted:	false
SSDEEP:	48:IwPGcprqGwpazG4pQrGrapbSTGQpKpG7HpRzTGIpG:rFZyQF6fBStAIT5A
MD5:	CB470FECF6A17D6FAA2BAAF9D7736E4C
SHA1:	837C2A92006B513699E00BF6CB2E081190BE9F5E
SHA-256:	BD05473CC4D77F0895DB86DEB385925478CA347A9A00AA413C24DCC0AB1E5DA7
SHA-512:	6E73CA4F6C6CF764C8F9DCB352DFDFA6D71008C529573BFF997279C58B258A789E7F715FCDE2C2BAF9DBC1E93EB692A319EF56169EF98CEDD1744B0480E251F
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):	853
Entropy (8bit):	7.159579117198893
Encrypted:	false
SSDEEP:	24:EwD7SByEH9bArPVO/XfF1NjjkJGHSE8ITh:EwD7SUEdsTgfd1eJGHrF
MD5:	400E7214932195470A141F321A70E4D4
SHA1:	A6B14168AF42FBE445CB9FEDF56C28F03D546E29
SHA-256:	D973815A9516947C6FCDE561C7868D6276181A92A3FD56C447298889D7C27485
SHA-512:	07B9A8217E25575B0C4B9A42DF253937D10CF67150FA2E196D221861E2B673359D2B365915F1AD5385C6D3AC20C89222825C698C49E515E23B00A718065EB7E1
Malicious:	false
Reputation:	low
Preview:	?.h.t.t.p.s.:././.w.w.w...g.o.o.g.l.e...c.o.m./.s.2./.f.a.v.i.c.o.n.s.?.d.o.m.a.i.n.=.d.e.l.l...c.o.m.?.v.=.B.U.I.L.D._.H.A.S.H.....PNG.....IHDR.....a....sBIT....|.d....hIDAT8...[H.a....&..0i.B.E`.YJ...Q.Mt..^H.B.;+\.D*K1...:8...B...7g....Xf.P..:.s.-.t...h/<7...^^..{...Z=..y.=pw.6zr....3.k..>.2.t.@.$...Bh..C...i6.D.=.HtN...>.....0.1.$..P.*3.I...Tf..Uf."...d...~....t.....$0..}T.._8>z..C.T..B.n.....Mb%B.n.t.l-.....sj.9ht...+.i..(.....k...Q..U^...V.$\..G.7&!...T.B...3UqQ.I....k*.4...2..... I.O.. dik.pD...Q$..&.IF./S(w...8{)...S.5.T....;....\|hu#....'C.NI.@@.+g.Qr.t~.....@..7....!.:.:..O..../."#LH...%...B..].a....*.....$KA.....".....".6p:.s .....h_..{.b.@.}]3...O$.+z.$.[#. ....]..&.e!&..mP.x..v...c+T..Pe.....v...:...v.y9...x.r|.`.3#…c...$#.O.(-i.2...>..._....IEND.B`.....4`.....4`....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\585b051251[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	10866
Entropy (8bit):	5.182477446178365
Encrypted:	false
SSDEEP:	192:BBHN42S+9SZRvACpiIthFzoXnemF+shSGnZ+PPxQDqv7jh81Q5l8OcchIlzbCn:HRCfhFzevnEZ/h81Q5l8OsE
MD5:	4B900F0AF3BBDA85E1077C8EC8C83831
SHA1:	7E7015965195F25AFA3A47BE2108278AD6A0A4AC
SHA-256:	7943D6D067DB8587E9FB675F0D2CC78D6C90C91B187CF8642A3F52FF91381685
SHA-512:	2CD82E0DCD1381447522CFFD6101365133323E5D2980FAE730801FE8BBA580FF7FDF9CB8D2E9AC794D6F2FB59C724EDA71BECE7CAA72C775BC963E1A54B30EBCB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://kit.fontawesome.com/585b051251.js
Preview:	window.FontAwesomeKitConfig = {"asyncLoading":{"enabled":true},"autoA11y":{"enabled":true},"baseUrl":"https://ka-f.fontawesome.com","baseUrlKit":"https://kit.fontawesome.com","detectConflictsUntil":null,"iconUploads":{},"id":132286382,"license":"free","method":"css","minify":{"enabled":true},"token":"585b051251","v4FontFaceShim":{"enabled":false},"v4shim":{"enabled":true},"version":"5.15.2"};.!function(t){"function"==typeof define&&define.amd?define("kit-loader",t):t()}((function(){"use strict";function t(e){return(t="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(t){return typeof t}:function(t){return t&&"function"==typeof Symbol&&t.constructor===Symbol&&t!==Symbol.prototype?"symbol":typeof t})(e)}function e(t,e,n){return e in t?Object.defineProperty(t,e,{value:n,enumerable:!0,configurable:!0,writable:!0}):t[e]=n,t}function n(t,e){var n=Object.keys(t);if(Object.getOwnPropertySymbols){var r=Object.getOwnPropertySymbols(t);e&&(r=r.filter((function(e){return Object.g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5309dd609ff4d2cc7b4d82702293091209e3ad38ed14aNHZVVml0czVCRkxRWmswVUVzPQ==UGFraXN0YW4=VUVzPQ==4vUVits5BFLQZk0[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	23818

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5309dd609ff4d2cc7b4d82702293091209e3ad38ed14aNHZVVml0czVCRkxRWmswVUVzPQ==UGFraXN0YW4=VUVzPQ==4vUVits5BFLQZk0[1].htm	
Entropy (8bit):	6.061224882394743
Encrypted:	false
SSDEEP:	384:Dwlk0vnywO1C3LGI0WDysoIAlwrtCN9by5Qkmcy77GAoIB44CGKM0k:8lk0BbPAv9b4kcyHfNB44D
MD5:	43BE1D7755FE24F913442C142E1A229A
SHA1:	124597C8C7ACD0FAEF8D50813AC7E02FBE52035E
SHA-256:	3FE6D8D257D4872091C96C553303C88A624A9EB59137693DF00FC261D337E550
SHA-512:	582D7E4A56CB5B9B3BBCF7E16DF2727D310F0BFF604430E2C83A461FBFF63983311282D0A9FB9DF5CF67A7FB466F6457925F4080D62706CAC532ACA2D815DAAE
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5309dd609ff4d2cc7b4d82702293091209e3ad38ed14aNHZVVml0czVCRkxRWmswVUVzPQ==UGFraXN0YW4=VUVzPQ==4vUVits5BFLQZk0[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://openplaywcowuk.gb.net/qwehbgfvdcfvtbgrvfecd/QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5309dd609ff4d2cc7b4d82702293091209e3ad38ed14aNHZVVml0czVCRkxRWmswVUVzPQ==UGFraXN0YW4=VUVzPQ==4vUVits5BFLQZk0/?Key=QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5309dd609ff4d2cc7b4d82702293091209e3ad38ed14aNHZVVml0czVCRkxRWmswVUVzPQ==UGFraXN0YW4=VUVzPQ==4vUVits5BFLQZk0&rand=13InboxLightaspxn_QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5309dd609ff4d2cc7b4d82702293091209e3ad38ed14aNHZVVml0czVCRkxRWmswVUVzPQ==UGFraXN0YW4=VUVzPQ==4vUVits5BFLQZk0_NHZVVml0czVCRkxRWmsw-&21613cde29049b3c91b62de76cfc8570a2e0ec37b8668ec5d246bab8a58db410
Preview:	..<!doctype html>..<html lang="en">..<head>.. <script src="https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>.. <script src="https://code.jquery.com/jquery-3.1.1.min.js">.. <script src="https://code.jquery.com/jquery-3.3.1.js" integrity="sha256-2Kok7MbOyxpgUVvAk/HJ2jigOSYS2auK4Pfzbm7uH60=" crossorigin="anonymous"></script>.. Required meta tags -->.. <meta charset="utf-8">.. <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">.. <link rel="icon" type="image/png" sizes="192x192" href="https://www.google.com/s2/favicons?domain=dell.com?v=BUILD_HASH">.... Bootstrap CSS -->.. <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css" integrity="sha384-Gn5384xqQ1aoWXA+058RXPxPg6fy4IWvTNh0E263XmFcJlSAwiGgFAW/dAiS6JXm" crossorigin="anonymous"> -->.. <link href="https://fonts.googleapis.com/css?family=Archivo+Narrow&display=swap" rel="stylesheet">.. <sc

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\favicons[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	653
Entropy (8bit):	7.583706692386441
Encrypted:	false
SSDEEP:	12:6v/7uNpP4+7ZHfiC6chzFbXpN2oXe4D+4HWWJdPdpdSrf6UsM1Zk4RHT6ND3Jj81:nTA6GqBbuoJj1rdSr6HqZkGTsj07
MD5:	A62D83D12160F4046567174039C651CE
SHA1:	677B914A00A3E9F5D1FA9850EFE477197D88DEAF
SHA-256:	1194ABC93F53E62EB6C8DD007F9D5E10F432CF97279A9E7C6DECC5815DC7F3A8
SHA-512:	60B2C99F1259D4BED96B6ADDC042FD1EF2E9A5C6D76B4F43211117976538FAADF86A687F3B3E82FDEB3A9E2D8C7B02629629693A5BDDB4BD000B5283DC1131B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/s2/favicons?domain=uottawa.ca
Preview:	.PNG.....IHDR.....h6....sBIT.....O....EIDAT(..RML.a.}.....K%E.P.BB..TP1x z..h4.....F0.`b...D..S=x.....H....%.C.....[.]v.K....T.....I.L.0".?.6=.k..}."lY..U...v.\_..o...^..}.5.2.c..#o....'...y.3ym...rC....i.|.....EJS....m.].W7~....(.#..vd&.D....`..L...:CD.....p.f.....O-....y.....S..IR...oHi....:..Xy.i..W.').`...H".....JK....\T...|..zKW..@geQ..`1k...&...q.../C.....pY...J..7^<.E...vX7*.+....{.dt.R.....P...cV:..oY.g...o...pt[.v.....dw.X..R....)8..n.mz2G..$....R....av~..=.^.m~...[e.s.....\...9.."d.Eiki..[%.+;.....(j.s.a.....I..h...bom.....p~..0...!_.u.....5.q.E.r.:.F.....O..\.4.3.=.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\free-v4-shims.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	26701
Entropy (8bit):	4.82979949483045
Encrypted:	false
SSDEEP:	192:SP6hT1bIl4w0QUmQ10PwKLaAu5CwWavpHo4O6wgLPbJVR8XD7mycP:5hal4w0QK+PwK05eavpmgPPeXD7mycP
MD5:	1848E71668F42835079E5FA2AF6CF4A8
SHA1:	6AE345E2FEB8C2A524E7CF9E22A3A87BAEE60593
SHA-256:	D7CC3C57F9BDA4C6DCB83BB3C19F2F2AA86ECEC6274E243CD4EC315AE8E30101
SHA-512:	24E0AF4EC32A9AAB61D9E1AF9B2083F2D13CC98961B5E32BB613A02FEEF63F5F30C3B21C6308A4A204D981D77C86F09E221D0DB7B051A3538ACE07E727F29F58
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.2/css/free-v4-shims.min.css?token=585b051251

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\free-v4-shims.min[1].css	
Preview:	/*!. * Font Awesome Free 5.15.2 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.fa.fa-glass:before{content:"\f000"}.fa.fa-meetup{font-family:"Font Awesome 5 Brands";font-weight:400}.fa.fa-star-o{font-family:"Font Awesome 5 F ree";font-weight:400}.fa.fa-star-o:before{content:"\f005"}.fa.fa-close:before,.fa.fa-remove:before{content:"\f00d"}.fa.fa-gear:before{content:"\f013"}.fa.fa-trash-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-trash-o:before{content:"\f2ed"}.fa.fa-file-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-file-o:before{co ntent:"\f15b"}.fa.fa-clock-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-clock-o:before{content:"\f017"}.fa.fa-arrow-circle-o-down{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arrow-circle-o-down:before{content:"\f358"}.fa.fa-arrow-circle-o-up{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arro

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\free.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	60351
Entropy (8bit):	4.728636851806783
Encrypted:	false
SSDEEP:	768:5Uh31IPiyXNq4YxBowbgJlkwF//zMQyYJYX9Bft6VSz8:5U0PxXE4YXJgndFTfy9lt5Q
MD5:	4ECC071B77D6B1790FA9FB8A5173F972
SHA1:	B44FCBAAC4F3AA7381D71DE20064AC84B0B729D1
SHA-256:	8C7BBA7DEB64FF95E98F7AC8CD0D3B675A4BCF02F302E57EDC5A1D6FA3D6CF94
SHA-512:	7CC1D04078B5917269025B6F37C7DDD83A0A5A0C5840E2A6E99ADFE2FB3E2242C626F25315480ADCD725C855AD2881DDF672B6FC1D793377C2D16FF38EAF69
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.2/css/free.min.css?token=585b051251
Preview:	/*!. * Font Awesome Free 5.15.2 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.fa,.fab,.fad,.fal,.far,.fas{-moz-osx-font-smoothing:grayscale;-webkit-font-smoothing:antialiased;display:inline-block;font-style:normal;font-var iant:normal;text-rendering:auto;line-height:1}.fa-lg{font-size:1.33333em;line-height:.75em;vertical-align:-.0667em}.fa-xs{font-size:.75em}.fa-sm{font-size:.875em}.fa-1x{font-size:1em}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-6x{font-size:6em}.fa-7x{font-size:7em}.fa-8x{font-size:8em}.fa-9x{font-size:9em}.fa-10x{font-size:10em}.fa-fw{text-align:center;width:1.25em}.fa-ul{list-style-type:none;margin-left:2.5em;padding-left:0}.fa-ul>li{position:relative}.fa-li{left:-2em;position:absolute;text-align:center;width:2em;line-height:inherit}.fa-border{border:.08em solid #eee;border-radius:.1em;padding:.2em .25em .15em}.fa-pul

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\KFOmCnqEu92Fr1Mu4mxM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20268, version 1.1
Category:	downloaded
Size (bytes):	20268
Entropy (8bit):	7.970212610239314
Encrypted:	false
SSDEEP:	384:LyfRPUY1e32pJd75q1DzPjsnouCrZsZtetWFNFfIP0clWvdzNcrm:uJPb1em3dSPjKrZYtWntk0wvdzh
MD5:	60FA3C0614B8FB2F394FA29944C21540
SHA1:	42C8AE79841C592A26633F10EE9A26C75BCF9273
SHA-256:	C1DC87F99C7FF228806117D58F085C6C573057FA237228081802B7D8D3CF7684
SHA-512:	C921362A52F3187224849EB566E297E48842D121E88C33449A5C6C1193FD4842BBD3EF181D770ADE9707011EB6F4078947B8165FAD51C72C17F43B592439FFF4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v20/KFOmCnqEu92Fr1Mu4mxM.woff
Preview:	wOFF.....O,.....P.....GDEF.....G...d....GPOS.....GSUB.....'.....r.OS/2.....P...`t...cmap...$.....W.cvt .....T...T+...fpgm...p...5....w.`.gasp..... ....glyf.....;Q..lD..&0hdmx..H....n..... ..head..Hx...6...6.j.zhhea..H.....$....hmtx..H....t.....Xdloca..KD.....BC%.maxp..M0... ... .(..name..MP.....t.U9.post..N ..... .m.dprep.. N4.....l.f..x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R...A.J.x.l..h.a.....l.m.6.1+.X....i...y....&...._..63..5....2>...x|D...ct.Kx..H@b.3..l..#u.....L.*.....^.*.4.....rP..{.* .....Q...JT.:Xu>..T./>...oq.....~..@.....lq../.... ..#..".&.8.H$..r...J)..jj...&..f.=.9..N9....'F..8.4.....m...m...m.m..n..&.X..}....S.|.....n.....PHaE...J*...4..MjJ.*..nW)..rn3'/.....ks5zY 5c...Mgg.5..p..rR{c...p..t\.8.c=..p...X.(.....7....=.....!...H .....(.0...(.q.JT?.b..z].'T...m..vNi.....t...:P.R..H....t.....&?.:.j.51+.S."j.SK'I.^....}S.i.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5309dd609ff4d2c c7b4d82702293091209e3ad38ed14aNHZVVml0czVCRkxRWmswVUVzPQ==UGFraXN0YW4=VUVzPQ==4vUVits5BFLQZk0[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):	850
Entropy (8bit):	5.7346673843137355
Encrypted:	false
SSDEEP:	24:y+OWPzaHwTAqrh+Isqrh+I9Aqrh+Ie4J5:0CNTJhBhjhS4J5
MD5:	EFFF4FF81E2E1FD1C325BB625FB687CF
SHA1:	E8D655F05532D3121B306359B6E68CC47C85A569
SHA-256:	97B6D4BEEA1C3B6B0358F6125957BA0778E4BDDAF879B4010D3D2CCE10B5968A
SHA-512:	C6C6F6503F22F177636ADCAD7AF2768889F9F38893EC71C1EDE4421B7488168FCC985E2A33E4207E8CE271A79AE6D004B86B599F77D6768B670C6B985428F8F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5309dd609ff4d2cc7b4d82702293091209e3ad38ed14aNHZVVml0czVCRkxRWmswVUVzPQ==UGFraXN0YW4=VUVzPQ==4vUVits5BFLQZk0[1].htm	
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\MEEXW4H4\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	223
Entropy (8bit):	5.142612311542767
Encrypted:	false
SSDEEP:	6:0IFFDK+Q+56ZRWHMqh7izlpdRSRk68k3tg9EFNin:jFI+QO6ZRoMqt6p3Tk9g9CY
MD5:	72C5D331F2135E52DA2A95F7854049A3
SHA1:	572F349BB65758D377CCBAE434350507341ACD7B
SHA-256:	C3A12D7E8F6B2B1F5E4CD0C9938DFC79532AEF90802B424EE910093F156586DA
SHA-512:	9EA12CC277C9858524083FEBBE1A3E61FDECE5268F63B14C9FFAFE29396C7CCDB3B07BE10E829936BCCD8F3B9E39DCFA6BC4316F189E4CEA914F1D06916DB66B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Archivo+Narrow&display=swap
Preview:	@font-face {. font-family: 'Archivo Narrow';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/archivonarrow/v12/tss0ApVBdCYD5Q7hcxTE1ArZ0bbwiXo.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\favicons[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	689
Entropy (8bit):	7.547514317403399
Encrypted:	false
SSDEEP:	12:6v/7aH90mJv85rPVOlNXbmMFb6IL9LjjPcQOJPQqG+GS+tVpAiz+1O4MbsDN:hH9bArPVO/XfF1NjjkJGHSE8ITG
MD5:	6F45B2E7280E12B8D0DF8280FDE4C155
SHA1:	7F4912503B0710270A047F0D1F2820FAE7B849E0
SHA-256:	B5BA52047193427D28D3F169FB3E4A2835C0FA1CA6F59192381BAA79CE74FBFB
SHA-512:	5C8C9114C682080337FD2BD2067D8C58C5E0D7E5B2DDEF64AE735E95AA5392AD15AE84153D7E15A113FF509B19B929616D74F5C65E2E583C2C7E3D122062F39
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a....sBIT....|.d....hIDAT8...[H.a....&..0i.B.E`.YJ...Q.Mt..^H.B.;+\.D*K1...:8...B...7g....Xf.P..:.s.-.t...h/<7...^^..{...Z=..y.=pw.6zr....3.k..>.2.t.@.$...Bh..C...i6.D.=.HtN...>.....0.1.$..P.*3.l...Tf..Uf."...d...~....t.......$0..}T.._8>z..C.T..B.n.....Mb%B.n.t.l-.....sj.9ht...+.i..(.....k...Q..U^...V.$\..G.7&!...T.B...3UqQ.l....k*.4...2..... I.O.. dik.pD...Q$..&.lF./S(w...8{)...S.5.T....;....\|hu#....'C.NI.@@.+g.Qr.t~.....@..7....!.:..:...O..../."#LH...%...B..].a....*.....$KA.....".....".6p:.s .....h_..{.b.@.}]3...O$.+z.$.[#. ....]..&.e!&..mP.x..v...c+T..Pe.....v...:...v.y9...x.r|.`.3#...c...$#.O.(-i.2...>..._....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\font-awesome.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	31000
Entropy (8bit):	4.746143404849733
Encrypted:	false
SSDEEP:	384:wHu5yWeTUKW+KlkJ5de2UYDyVfwYUas2l8yQ/8dwmaU8G:wwlr+Klk3Yi+fwYUf2l8yQ/e9vf
MD5:	269550530CC127B6AA5A35925A7DE6CE
SHA1:	512C7D79033E3028A9BE61B540CF1A6870C896F8
SHA-256:	799AEB25CC0373FDEE0E1B1DB7AD6C2F6A0E058DFADAA3379689F583213190BD
SHA-512:	49F4E24E55FA924FAA8AD7DEBE5FFB2E26D439E25696DF6B6F20E7F766B50EA58EC3DBD61B6305A1ACACD2C80E6E659ACCEE4140F885B9C9E71008E9001FBF4B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://firebasestorage.googleapis.com/v0/b/dellcssfile.appspot.com/o/font-awesome.min.css?alt=media&token=e6f19ce7-a9ca-457e-80df-0f4823412ad5

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\font-awesome.min[1].css	
Preview:	/*! * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */@font-face{font-family:'FontAwesome';src:url('../fonts/fontawesome-webfont.eot?v=4.7.0');src:url('../fonts/fontawesome-webfont.eot?#iefix&v=4.7.0') format('embedded-opentype'),url('../fonts/fontawesome-webfont.woff2?v=4.7.0') format('woff2'),url('../fonts/fontawesome-webfont.woff?v=4.7.0') format('woff'),url('../fonts/fontawesome-webfont.ttf?v=4.7.0') format('truetype'),url('../fonts/fontawesome-webfont.svg?v=4.7.0#fontawesomeregular') format('svg');font-weight:normal;font-style:normal}.fa{display:inline-block;font:normal normal normal 14px/1 FontAwesome;font-size:inherit;text-rendering:auto;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.fa-lg{font-size:1.33333333em;line-height:.75em;vertical-align:-15%}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-fw{width:1.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\mem8YaGs126MiZpBA-UFVZ0d[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18100, version 1.1
Category:	downloaded
Size (bytes):	18100
Entropy (8bit):	7.962027637722169
Encrypted:	false
SSDEEP:	384:aHQHZuiZQFFIimUy1oml4hN2Vmw1Qa57YC74ObDDj08X0UJQiXc:1ZQT0UySml4bEmAP5EC7PbDH4U1M
MD5:	DE0869E324680C99EFA1250515B4B41C
SHA1:	8033A128504F11145EA791E481E3CF79DCD290E2
SHA-256:	81F0EC27796225EA29F9F1C7B74F083EDCD7BC97A09D5FC4E8D03C0134E62445
SHA-512:	CD616DB99B91C6CBF427969F715197D54287BAFA60C3B58B93FF7837C21A6AAC1A984451AEEB9E07FD5B1B0EC465FE020ACBE1BFF8320E1628E970DDF37B0F0E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem8YaGs126MiZpBA-UFVZ0d.woff
Preview:	wOFF.....F.....i.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....^...`~]..cmap...`.....X..cvt .....Y.....M..fpgm...p.....~a..gasp.....#glyf.....6...S...]head..>....6...6..cphhea..>.....$....hmtx..?.....[$loca..A4.....f..maxp..B.... .. ....name..C.....&:A.post..D.....x.U..prep..E.....C.....x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`f..8.....u..1...<.f.....A.....5....1...A.._6..".-..L.....Ar,.....3..(....x.\.!..q.....#aff...#1Q@.'U..@5."..llt.Aa#.f|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..l;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$KY...e@.,.."..........?....%.g....Z.....(".o..Y..Bu342.e.....0.....M=.....x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...s.3.S...co..o.~.Zy.u...kW.\.t...N.KG.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\popper.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	19188
Entropy (8bit):	5.212814407014048
Encrypted:	false
SSDEEP:	384:+CbuG4xGNoDic2UjKPafxwC5b/4xQviOJU7QzxzivDdE3pcGdjkd/9jt3B+Kb964:zb4xGmiJfaf7gxQvVU7eziv+cSjknZ3f
MD5:	70D3FDA195602FE8B75E0097EED74DDE
SHA1:	C3B977AA4B8DFB69D651E07015031D385DED964B
SHA-256:	A52F7AA54D7BCAAFA056EE0A050262DFC5694AE28DEE8B4CAC3429AF37FF0D66
SHA-512:	51AFFB5A8CFD2F93B473007F6987B19A0A1A0FB970DDD59EF45BD77A355D82ABBBD60468837A09823496411E797F05B1F962AE93C725ED4C00D514BA40269D1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js
Preview:	/*. Copyright (C) Federico Zivolo 2017. Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT).. */(function(e,t){'object'==typeof exports&&'undefined'!=typeof module?module.exports=t():'function'==typeof define&&define.amd?define(t):e.Popper=t()})(this,function(){'use strict';function e(e){return e&&'[object Function]'==={}.toString.call(e)}function t(e,t){if(1!==e.nodeType)return[];var o=getComputedStyle(e,null);return t?o[t]:o}function o(e){return'HTML'===e.nodeName?e:e.parentNode||e.host}function n(e){if(!e)return document.body;switch(e.nodeName){case'HTML':case'BODY':return e.ownerDocument.body;case'#document':return e.body;}var i=t(e),r=i.overflow,p=i.overflowX,s=i.overflowY;return /(auto|scroll)/.test(r+s+p)?e:n(o(e))}function r(e){var o=e&&e.offsetParent,i=o&&o.nodeName;return i&&'BODY'!==i&&'HTML'!==i?-1!==['TD','TABLE'].indexOf(o.nodeName)&&'static'===t(o,'position')?r(o):o:e?e.ownerDocument.documentElement:document.documentElement}functio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\qwehbgfvdcfvtbgrvfecd[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	1159
Entropy (8bit):	5.13059579294646
Encrypted:	false
SSDEEP:	12:cqJmrAKPqrh+kcAUISiIXW9lYiIy8i4CwvijFCEVoYOwJ22OX4xxQFL3TPxnuYTB:D5Wqrh+lUISiI2lYiIyhLXdP+oYwBgb
MD5:	EA9AB1F2067E529B014DD4A5E0D5E84F
SHA1:	99D46F4B5823074E2FAC99F6309C09ADC186811B
SHA-256:	B2D54A1272F3D3C2EEC08C22B630BF2559586BE365F30246563A8014C232957F
SHA-512:	095FF769FA7CA923F349F22A057E524A4D9570D1485892669F1C7959F84C6265191A3373B661B3DF331864C4EF959F083C010F4E4266A6797CC8FAD211A2926C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\qwehbgfvdcfvtbgrvfecd[1].htm	
Preview:	.<script type="text/javascript">.. var random = 'QXNpYQ==22-02-202107-56-25pm3803fe4e995ba53820d5309dd609ff4d2cc7b4d82702293091209e3ad38e d14aNHZVVml0czVCRkxRWmswVUVzPQ==UGFraXN0YW4=VUVzPQ==4vUVits5BFLQZk0';. var b = 'NHZVVml0czVCRkxRWmsw';. var result = '21613c de29049b3c91b62de76cfc8570a2e0ec37b8668ec5d246bab8a58db410';. var url = "";.. var hashValue = location.hash.substr(1);. if (hashValue == "") {. var queryString = window.location.search;. var urlParams = new URLSearchParams(queryString);. var userid = urlParams.get('userid');.. if (userid != "" && useri d != null) {. url = random + "?Key=" + random + "&rand=13InboxLightaspxn_" + random + "_" + b + "-&" + result + "&userid=" + userid;. window.location.href = url;. } else {. url = random + "?Key=" + random + "&rand=13InboxLightaspxn_" + random + "_" + b + "-&" + result;. window.location.href = url;.. }.. } else {. url = ra

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	726
Entropy (8bit):	5.180796546063191
Encrypted:	false
SSDEEP:	12:jFMO6ZRoT6pIFqFMO6ZN76pYnJqF/iO6ZRoT6pixuGEqF/iO6ZN76pixuyvJY:5MOYsiMOYN7q/iOYsNxDv/iOYN7Nxw
MD5:	22502A622488078B8DE4406FD548E1E5
SHA1:	78475040F2A19CE19AE97F70AB5086C52161F707
SHA-256:	37EFD16EBE120F8057C19B36BE006601E83EB64772A25897E07293891C4F3BC0
SHA-512:	D03E79E23C2CBC8017CF43CF24A57DE4397CC58EC6291070E8E96998670F8DC42394709C5DC38B03199D3AE8E2A40563A5E3A41DC4148859A7FB472137991625
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/opensans/v18/mem8YaGs126MiZpBA-UFVZ0d.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN7rgOUuhv.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/roboto/v20/KFOmCnqEu92Fr1Mu4mxM.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/roboto/v20/KFOlCnqEu92Fr1MmWUlfBBc-.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\free-fa-regular-400[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Font Awesome 5 Free Regular family
Category:	downloaded
Size (bytes):	34350
Entropy (8bit):	6.319416398409097
Encrypted:	false
SSDEEP:	384:2TILSQt3owpXUazLuDULbNVTH/oOkKQB3I+89AyI6WcRwkw8cQUtR:2ULSe3yy6DOP/oDB29uc5w8cQUL
MD5:	73570FCA80D5237954C19C20BDA58A70
SHA1:	E27F09071CA6B858A1B96B1CD02B2B34BCE85178
SHA-256:	75BAC9C568E4B2DF8C25F96513A92FA4740D4B11E58FB0ADB88E2F4DADC7FFCD
SHA-512:	60632D9B3893631C82FDC7D56741A8EFA52BA9333BF4FECA083330B9B1454CC6F4A1AEEDF621EBF92CFF634A0BA91F4EB1F0DF6009A69C6BD14A0A39908E8B 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.2/webfonts/free-fa-regular-400.eot?
Preview:	.....LP.....w.....6.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .R.e.g.u.l.a.r.....R.e.g.u.l.a.r...L.3.3.1...5.2.2. .(.F.o.n.t. .A.w.e.s.o.m.e. .v.e.r. s.i.o.n.:. .5...1.5...2.)...6.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .R.e.g.u.l.a.r.....PFFTM.4.....GDEF.*.....OS/2A.S....X...`cmap.....gasp.....glyf|.7.... ..n.head.& .....6hhea.5.....$hmtx...t.....Tloca.e.....6maxp.....8... name9.;"..w....[post.iA...}.....K...w.._.<.....$.Z.....$.`..... ..@.....L.f...G.L.f.....PfEd.....T.....:..... .....@.....@.....@.....@.....@...@.....@...@..... .....`.....@.....@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\jquery-3.1.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	86709
Entropy (8bit):	5.367391365596119
Encrypted:	false
SSDEEP:	1536:9NhEyjjTikEJO4edXXe9J578go6MWXqcVhrLyB4Lw13sh2bzrl1+iuH7U3gBORDT:jxcq0hrLZwpsYbmzORDU8Cu5
MD5:	E071ABDA8FE61194711CFC2AB99FE104
SHA1:	F647A6D37DC4CA055CED3CF64BBC1F490070ACBA
SHA-256:	85556761A8800D14CED8FCD41A6B8B26BF012D44A318866C0D81A62092EFD9BF
SHA-512:	53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D69067E 65
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.1.1.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\jquery-3.1.1.min[1].js	
Preview:	/*! jQuery v3.1.1 | (c) jQuery Foundation | jquery.org/license */!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.1.1",r=function(a,b){return new r.fn.init(a,b)},s=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,t=/^-ms-/,u=/-([a-z])/g,v=function(a,b){return b.toUpperCase()};r.fn=r.prototype={jquery:q,constructor:r,length:0,toArray:function(){return f.call(this)},get:function(a){return null==a?f.call(this):a<0?this[a+this.length]:this[a]},pushStack:function(a){var b=r.merge(this.con

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\jquery-3.2.1.slim.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	69597
Entropy (8bit):	5.369216080582935
Encrypted:	false
SSDEEP:	1536:qNhEyjjTikEJO4edXXe9J578go6MWX2xkjVe4c4j2ll2Ac7pK3F71QDU8CuT:Exc2yjq4j2uYnQDU8CuT
MD5:	5F48FC77CAC90C4778FA24EC9C57F37D
SHA1:	9E89D1515BC4C371B86F4CB1002FD8E377C1829F
SHA-256:	9365920887B11B33A3DC4BA28A0F93951F200341263E3B9CEFD384798E4BE398
SHA-512:	CAB8C4AFA1D8E3A8B7856EE29AE92566D44CEEAD70C8D533F2C98A976D77D0E1D314719B5C6A473789D8C6B21EBB4B89A6B0EC2E1C9C618FB1437EBC77D3A269
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.2.1.slim.min.js
Preview:	/*! jQuery v3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_evalUrl,-event/ajax,-effects,-effects/Tween,-effects/animatedSelector | (c) JS Foundation and other contributors | jquery.org/license */!function(a,b){"use strict";"object"==typeof module &&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_e

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\KFOlCnqEu92Fr1MmWUlfBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20356, version 1.1
Category:	downloaded
Size (bytes):	20356
Entropy (8bit):	7.972919215442608
Encrypted:	false
SSDEEP:	384:of+dt1ebKR28EPpAXxR5wthZZv4B8Te/h4+ctr5NH9NwZaUp4VsEgm:of+P1eeRcU8Hqdy+UHHbEw/
MD5:	ADCDE98F1D584DE52060AD7B16373DA3
SHA1:	0A9B76D81989A7A45336EBD7B48ED25803F344B9
SHA-256:	806EA46C426AF8FC24E5CF42A210228739696933D36299EB28AEE64F69FC71F1
SHA-512:	7B1D6CC0D841A9E5EFEC540387BC5F9B47E07A21FDC3DC4CE029BB0E3C74664BBC9F1BCCFD8FB575B595C2CC1FD16925C533E062C4C82EEE0C310FFD2B4C927
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\KFOlCnqEu92Fr1MmWUlfBBc-[1].woff	
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v20/KFOlCnqEu92Fr1MmWUlfBBc-.woff
Preview:	wOFF.....O.....GDEF.....G...d....GPOS.....~..GSUB.....'.....r.OS/2.....Q...`u...cmap...\.....W.cvt ...T...H...H+~..fpgm.....3...._...gasp..... ....glyf.....;...k....hdmx..H....m....!$..head..H....6...6...\hhea..I,.....$.&..hmtx..IL...y.....XF.loca..K.....`.C.maxp..M.... ... .(..name..M.....~..9.post..N..... .m.dprep..N.....)* v60x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R...A.J.x....dK...{....?..F?.|.~.m...ms.{.Z..;.....U.]7s.....\.=D.=.7...>....x...D..O|.U:...|o..3.x.j.r"B..... .1LGmaGxQxG....~.:'.A..hd.z,.k..KO.....^.}H|#z_.O.....R..A...9..A..!.(./...".:.Iq1.r..s..r.7r.7s..q.wr....nz..]...2..d4c..c....d....T.1...d....\....,c9k.g..Yv.#O."%..... ...t"uM..%..... j.#^.....}\c.q.i...<jy.D...C.01.2.r.....V..z.W.7b..L.S.41]..kUs.X/6..b.....(..(...K..{.^..'.....`#./..B.....N+p.m`...].IQ....Drg.M..Kx.^.S.*.....h ..$.k.'Hy.I.ze..4z.-T.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	121200
Entropy (8bit):	5.0982146191887106
Encrypted:	false
SSDEEP:	768:Vy3Gxw/Vc/QWlJxtQOIuiHlq5mzI4X8OAduFKbv2ctg2Bd8JP7ecQVvH1FS:nw/a1fIuiHlq5mN8lDbNmPbh
MD5:	EC3BB52A00E176A7181D454DFFAEA219
SHA1:	6527D8BF3E1E9368BAB8C7B60F56BC01FA3AFD68
SHA-256:	F75E846CC83BD11432F4B1E21A45F31BC85283D11D372F7B19ACCD1BF6A2635C
SHA-512:	E8C5DAF01EAE68ED7C1E277A6E544C7AD108A0FA877FB531D6D9F2210769B7DA88E4E002C7B0BE3B72154EBF7CBF01A795C8342CE2DAD368BD6351E956195F 8B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://firebasestorage.googleapis.com/v0/b/dellcssfile.appspot.com/o/bootstrap.min.css?alt=media&token=ec34bc68-b721-48e5-a02a-8deed9a44325
Preview:	/*!. * Bootstrap v3.3.7 (http://getbootstrap.com). * Copyright 2011-2016 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */html{font-family:sans-serif;-webkit-text-size-adjust:100%;-ms-text-size-adjust:100%}body{margin: 0}article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align :baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background-color:transparent}a:active,a:hover{outline:0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:700}dfn{font-style:italic}h1{margin:.67em 0;font-size:2em}mark{color:#000;background:#ff0}small{font-size:80%}sub,sup{position:relative;font- size:75%;line-height:0;vertical-align:baseline}sup{top:-.5em}sub{bottom:-.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\bootstrap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	51039
Entropy (8bit):	5.247253437401007
Encrypted:	false
SSDEEP:	768:E9Yw7GuJM+HV0cen/7Kh5rM7V4RxCKg8FW/xsXQUd+FiID65r48Hgp5HRl+:E9X7PMIM7V4R5LFAxTWyuHHgp5HRl+
MD5:	67176C242E1BDC20603C878DEE836DF3
SHA1:	27A71B00383D61EF3C489326B3564D698FC1227C
SHA-256:	56C12A125B021D21A69E61D7190CEFA168D6C28CE715265CEA1B3B0112D169C4
SHA-512:	9FA75814E1B9F7DB38FE61A503A13E60B82D83DB8F4CE30351BD08A6B48C0D854BAF472D891AF23C443C8293380C2325C7B3361B708AF9971AA0EA09A25CDD0 A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v4.1.3 (https://getbootstrap.com/). * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed un der MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jque ry"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,h){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}funct ion s(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function l(r){for(var t=1;t<arguments.length;t++){var o=null!=arguments[t]?arguments[t]:{},e=Object.keys(o);"function" ==typeof Object.getOwnPropertySymbols&&(e=e.concat(Object.getOwnPropertySymbols(o).filter(function(t){return Object.getOwnPropertyDescriptor(o,t).enum

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\bootstrap.min[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	48944
Entropy (8bit):	5.272507874206726
Encrypted:	false
SSDEEP:	768:9VG5R15WbHVKZrycEHSYro34CrSLB6WU/6DqBf4l1B:9VIRuo53XiwWTvl1B
MD5:	14D449EB8876FA55E1EF3C2CC52B0C17
SHA1:	A9545831803B1359CFEED47E3B4D6BAE68E40E99
SHA-256:	E7ED36CEEE5450B4243BBC35188AFABDFB4280C7C57597001DE0ED167299B01B
SHA-512:	00D9069B9BD29AD0DAA0503F341D67549CCE28E888E1AFFD1A2A45B64A4C1BC460D81CFC4751857F991F2F4FB3D2572FD97FCA651BA0C2B0255530209B182F2
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\bootstrap.min[2].js	
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,n){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function s(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function r(){return(r=Object.assign||function(t){for(var e=1;e<arguments.length;e++){var n=arguments[e];for(var i in n)Object.prototype.hasOwnProperty.call(n,i)&&(t[i]=n[i])}return t}).apply(this,arguments)}e=e&&e.hasOwnProperty("default")?e.default:e,n=n&&n.hasOwnProp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\free-fa-solid-900[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Font Awesome 5 Free Solid family
Category:	downloaded
Size (bytes):	204814
Entropy (8bit):	6.343269877413605
Encrypted:	false
SSDEEP:	6144:9t+zd6McnODzpN2BDXTIRSwRKSK3NC59M4:iELnODze58Rjg+5b
MD5:	AD5381B40F2857CE48DC73585FC92294
SHA1:	B404BB9916EDFD272560C27CFD09C032EC9F9B96
SHA-256:	2D45F4A3844BEFB918111DF65049A4FA71577D5E8FF009934B62E647E4702AB0
SHA-512:	69409725FE954403937CA22F5CDE811574FA2EBDBE24BF7CD5566826259A2427692251BFC90E663696C6A425F6C2DB95C8946495B4A5228B3BA8FEA10F79C2F5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.2/webfonts/free-fa-solid-900.eot?
Preview:	. .....LP.....F.....2.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .S.o.l.i.d.....S.o.l.i.d...L.3.3.1...5.2.2. .(.F.o.n.t. .A.w.e.s.o.m.e. .v.e.r.s.i.o.n.:. .5...1.5...2.)...2.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .S.o.l.i.d.....PFFTM.4.....GDEF.*.....OS/23.V`...X...`cmap.j.4...h....gasp.....glyfh.....-....dhead.4.....6hhea.C.-....$hmtx.Q.....loca.....8....maxp.N.`...8... name#./....P...+post..Fa...|..1.....K..F..._.<.....$.\.....$.`.....]. .....@..... L.f...G.L.f.....PfEd.....T.....:.... .....@.....@. .....@.....@.....@.....`.....@.....@.....@.....@....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\mem5YaGs126MiZpBA-UN7rgOUuhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18900, version 1.1
Category:	downloaded
Size (bytes):	18900
Entropy (8bit):	7.96514104643824
Encrypted:	false
SSDEEP:	384:nejx4dDcsFhu/3v79dEAUdH6XSw1fz9fKQm9LQNG/X1epB:ejadDrhYTf3Udaieza98Nbz
MD5:	1F85E92D8FF443980BC0F83AD7B23B60
SHA1:	EE8642C4FAE325BB460EC29C0C2C9AD8A4C7817D
SHA-256:	EA20E5DB3BA915C503173FAE268445FC2745FC9A5DCE2F58D47F5A355E1CDB18
SHA-512:	F34099C30F35F782C8BB2B92D7F44549013D90E9EEDE13816D4C7380147D5B2C8373CC4D858CDF3248AAA8A73948350340EE57DAE9734038FC80615848C7133E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN7rgOUuhv.woff
Preview:	wOFF.....l.....p.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....^...`....cmap...`.....X..cvt .....]....-...fpgm...t.....s.ugasp.....glyf...$ ..9...Y..(.head..A....6...6.%l.hhea..B,.....$.)..hmtx..BL.....O,loca..D`.....9yfmaxp..F$... ... .q..name..FD.....#.>.post..G4.....x.U..prep..H.....k..... .....x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`f.g.....:....Q.B3_dHc.....@`...../..?....^..... 9.8.m@J....w..!..x.\.!..q.....#aff...#1Q@ .'U..@5.".llt.Aa#.f\c.W....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e(}.IS2..uc]p.....M.x.c.a.g``..$KY...e@.,q@.j...o@<..O.H.t..... .....c .p@.....3lbd.....-.}.M...!...!....x.TGw.F.....)..)7.W..`*.j.-...=*'_..sl...2...O>....[tt....TK]..|...G.....^.m..=..x.q...+./].p...

C:\Users\user\AppData\Local\Temp\~DF5C6855DB7C39EC1D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	67554
Entropy (8bit):	1.6279134946883764
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+QWMNWb1bcN1bczRDRHE5KKBalyHBLMyKKBalyHBLMRm66Lml6:kBqoxKAuqR+QWMNW5b8bopt3fyY
MD5:	4397A6AC09441CFB762974D0CFF0741B
SHA1:	555D166A1A7441598E506D9BF32FFF6679A611B7
SHA-256:	F425D26FAB1E115B3F21CBCDFE53BDE0EC97348E82D8959BFF837EBDF6C3CD06
SHA-512:	304BECA5B802AEE084C94975087D4152DE47867D64AC00C9D3BEB25880925E1483D3B906F945EDDFD72B6A4066744B7BE9B2C57F825F6B97436872B667F191C4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DF5C6855DB7C39EC1D.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFD7E45C6E89F63922.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.481141681285755
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo/YF9lo/g9lW/NohmoA:kBqoI/r/N/NohmoA
MD5:	B5A9215D05744CA7B1776A14523A6654
SHA1:	F09ED003F9E2DA7291C2012A33D2DBE9124D0B32
SHA-256:	E005D2CE7F7323AAC3AFC7F03634F7A93317EC9827D49453B845A8066FD1ABE1
SHA-512:	E823DECAE6EFAA96F921D31BE8EE48E2F7AA76E6A2ADC26CE43128E092A103568F2AA956020CC989906095B712F5E8E2F4DFC553CF244305084D9CE3A456D69 D
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFDD76AF591DFFF30C.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...(.................. ....

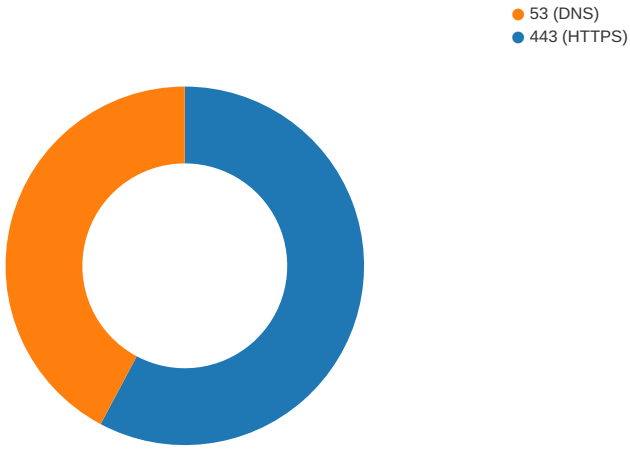
Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 90



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:56:23.903907061 CET	49716	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:23.904026985 CET	49715	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:24.059267998 CET	443	49716	173.237.190.111	192.168.2.3
Feb 22, 2021 20:56:24.059317112 CET	443	49715	173.237.190.111	192.168.2.3
Feb 22, 2021 20:56:24.059431076 CET	49716	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:24.059561968 CET	49715	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:24.065181017 CET	49715	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:24.065222979 CET	49716	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:24.220138073 CET	443	49715	173.237.190.111	192.168.2.3
Feb 22, 2021 20:56:24.220267057 CET	443	49716	173.237.190.111	192.168.2.3
Feb 22, 2021 20:56:24.224426985 CET	443	49716	173.237.190.111	192.168.2.3
Feb 22, 2021 20:56:24.224467039 CET	443	49716	173.237.190.111	192.168.2.3
Feb 22, 2021 20:56:24.224509001 CET	443	49716	173.237.190.111	192.168.2.3
Feb 22, 2021 20:56:24.224674940 CET	49716	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:24.224745035 CET	443	49715	173.237.190.111	192.168.2.3
Feb 22, 2021 20:56:24.224793911 CET	443	49715	173.237.190.111	192.168.2.3
Feb 22, 2021 20:56:24.224828005 CET	443	49715	173.237.190.111	192.168.2.3
Feb 22, 2021 20:56:24.224898100 CET	49715	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:24.224945068 CET	49715	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:24.261940956 CET	49715	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:24.262036085 CET	49716	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:24.269485950 CET	49716	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:24.269659996 CET	49715	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:24.269680023 CET	49716	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:24.419209003 CET	443	49715	173.237.190.111	192.168.2.3
Feb 22, 2021 20:56:24.419248104 CET	443	49716	173.237.190.111	192.168.2.3
Feb 22, 2021 20:56:24.419450045 CET	443	49715	173.237.190.111	192.168.2.3
Feb 22, 2021 20:56:24.419451952 CET	49715	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:24.419559002 CET	49716	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:24.419563055 CET	49715	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:24.419601917 CET	443	49716	173.237.190.111	192.168.2.3
Feb 22, 2021 20:56:24.419694901 CET	49716	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:24.421212912 CET	49716	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:24.421336889 CET	49715	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:24.426117897 CET	443	49715	173.237.190.111	192.168.2.3
Feb 22, 2021 20:56:24.426147938 CET	443	49716	173.237.190.111	192.168.2.3
Feb 22, 2021 20:56:24.426242113 CET	49715	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:24.426589966 CET	443	49716	173.237.190.111	192.168.2.3
Feb 22, 2021 20:56:24.426728964 CET	49716	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:24.615251064 CET	443	49716	173.237.190.111	192.168.2.3
Feb 22, 2021 20:56:24.615369081 CET	49716	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:24.616722107 CET	443	49715	173.237.190.111	192.168.2.3
Feb 22, 2021 20:56:24.828483105 CET	49716	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:24.976794004 CET	49718	443	192.168.2.3	104.129.25.9

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:56:24.977623940 CET	49719	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:24.993236065 CET	443	49716	173.237.190.111	192.168.2.3
Feb 22, 2021 20:56:24.993316889 CET	49716	443	192.168.2.3	173.237.190.111
Feb 22, 2021 20:56:25.118632078 CET	443	49718	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:25.118760109 CET	49718	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:25.119131088 CET	443	49719	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:25.119288921 CET	49719	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:25.119646072 CET	49718	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:25.120569944 CET	49719	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:25.261374950 CET	443	49718	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:25.262279987 CET	443	49719	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:25.262685061 CET	443	49718	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:25.262758017 CET	443	49718	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:25.262785912 CET	49718	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:25.262789011 CET	443	49718	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:25.262819052 CET	443	49718	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:25.262846947 CET	49718	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:25.262876987 CET	49718	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:25.264277935 CET	443	49719	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:25.264322042 CET	443	49719	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:25.264350891 CET	443	49719	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:25.264375925 CET	443	49719	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:25.264394999 CET	49719	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:25.264455080 CET	49719	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:25.264468908 CET	49719	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:25.271015882 CET	49718	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:25.271538019 CET	49718	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:25.274363041 CET	49719	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:25.414917946 CET	443	49718	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:25.414968967 CET	443	49718	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:25.415096998 CET	49718	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:25.418068886 CET	443	49719	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:25.418175936 CET	49719	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:25.644025087 CET	443	49718	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:25.644049883 CET	443	49718	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:25.644172907 CET	49718	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:25.728319883 CET	49718	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:25.872622013 CET	443	49718	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:25.872668982 CET	443	49718	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:25.872720957 CET	49718	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:25.872767925 CET	49718	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:25.876589060 CET	49718	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:26.019649982 CET	443	49718	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:26.019702911 CET	443	49718	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:26.019727945 CET	443	49718	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:26.019737959 CET	49718	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:26.019774914 CET	443	49718	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:26.019783020 CET	49718	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:26.019819021 CET	443	49718	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:26.019829988 CET	49718	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:26.019846916 CET	443	49718	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:26.019879103 CET	49718	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:26.019885063 CET	443	49718	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:26.019925117 CET	443	49718	104.129.25.9	192.168.2.3
Feb 22, 2021 20:56:26.019938946 CET	49718	443	192.168.2.3	104.129.25.9
Feb 22, 2021 20:56:26.019949913 CET	443	49718	104.129.25.9	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:56:16.330821037 CET	64938	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:16.382500887 CET	53	64938	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:17.081979990 CET	60152	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:17.133752108 CET	53	60152	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:56:17.874104977 CET	57544	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:17.922708035 CET	53	57544	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:18.627623081 CET	55984	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:18.679543972 CET	53	55984	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:19.453756094 CET	64185	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:19.502549887 CET	53	64185	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:20.406322956 CET	65110	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:20.458750010 CET	53	65110	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:21.240645885 CET	58361	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:21.297796011 CET	53	58361	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:22.194928885 CET	63492	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:22.252252102 CET	53	63492	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:22.697314024 CET	60831	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:22.755914927 CET	53	60831	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:22.973278999 CET	60100	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:23.022108078 CET	53	60100	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:23.711832047 CET	53195	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:23.895539045 CET	53	53195	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:23.918183088 CET	50141	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:23.966948986 CET	53	50141	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:24.899224043 CET	53023	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:24.923929930 CET	49563	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:24.956496000 CET	53	53023	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:24.975552082 CET	53	49563	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:26.177388906 CET	51352	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:26.183619976 CET	59349	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:26.191047907 CET	57084	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:26.208959103 CET	58823	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:26.218769073 CET	57568	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:26.232407093 CET	53	59349	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:26.238873959 CET	50540	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:26.244573116 CET	54366	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:26.248070002 CET	53	51352	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:26.251395941 CET	53034	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:26.257582903 CET	53	58823	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:26.258510113 CET	53	57084	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:26.277654886 CET	57762	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:26.283724070 CET	53	57568	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:26.287740946 CET	53	50540	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:26.293267965 CET	53	54366	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:26.299892902 CET	53	53034	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:26.329796076 CET	53	57762	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:26.654263020 CET	55435	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:26.703097105 CET	53	55435	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:27.350933075 CET	50713	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:27.402702093 CET	53	50713	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:27.910645962 CET	56132	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:27.972641945 CET	53	56132	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:28.297825098 CET	58987	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:28.358324051 CET	53	58987	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:30.326498032 CET	56579	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:30.378040075 CET	53	56579	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:31.420686960 CET	60633	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:31.472698927 CET	53	60633	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:32.188550949 CET	61292	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:32.237518072 CET	53	61292	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:40.803025007 CET	63619	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:40.860398054 CET	53	63619	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:42.827167034 CET	64938	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:42.940218925 CET	53	64938	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:43.384928942 CET	61946	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:43.449754953 CET	53	61946	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:49.144385099 CET	64910	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:49.193274975 CET	53	64910	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:56:52.687418938 CET	52123	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:52.736247063 CET	53	52123	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:53.370122910 CET	56130	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:53.422729969 CET	53	56130	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:53.693512917 CET	52123	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:53.742299080 CET	53	52123	8.8.8.8	192.168.2.3
Feb 22, 2021 20:56:53.785799980 CET	56338	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:56:53.844521999 CET	53	56338	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 20:56:23.711832047 CET	192.168.2.3	8.8.8.8	0x9790	Standard query (0)	architectc hintanvirani.com	A (IP address)	IN (0x0001)
Feb 22, 2021 20:56:24.899224043 CET	192.168.2.3	8.8.8.8	0x789e	Standard query (0)	openplaywc owuk.gb.net	A (IP address)	IN (0x0001)
Feb 22, 2021 20:56:26.183619976 CET	192.168.2.3	8.8.8.8	0x1c36	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Feb 22, 2021 20:56:26.208959103 CET	192.168.2.3	8.8.8.8	0x51e7	Standard query (0)	kit.fontaw esome.com	A (IP address)	IN (0x0001)
Feb 22, 2021 20:56:26.238873959 CET	192.168.2.3	8.8.8.8	0xa837	Standard query (0)	cdnjs.clou dflare.com	A (IP address)	IN (0x0001)
Feb 22, 2021 20:56:26.244573116 CET	192.168.2.3	8.8.8.8	0x71c2	Standard query (0)	maxcdn.boo tstrapcdn.com	A (IP address)	IN (0x0001)
Feb 22, 2021 20:56:26.251395941 CET	192.168.2.3	8.8.8.8	0x322a	Standard query (0)	stackpath. bootstrapc dn.com	A (IP address)	IN (0x0001)
Feb 22, 2021 20:56:26.654263020 CET	192.168.2.3	8.8.8.8	0x4146	Standard query (0)	ka-f.fonta wesome.com	A (IP address)	IN (0x0001)
Feb 22, 2021 20:56:42.827167034 CET	192.168.2.3	8.8.8.8	0xe83f	Standard query (0)	www.politi kesgeuseis.gr	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 20:56:23.895539045 CET	8.8.8.8	192.168.2.3	0x9790	No error (0)	architectc hintanvirani.com		173.237.190.111	A (IP address)	IN (0x0001)
Feb 22, 2021 20:56:24.956496000 CET	8.8.8.8	192.168.2.3	0x789e	No error (0)	openplaywc owuk.gb.net		104.129.25.9	A (IP address)	IN (0x0001)
Feb 22, 2021 20:56:26.232407093 CET	8.8.8.8	192.168.2.3	0x1c36	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 20:56:26.257582903 CET	8.8.8.8	192.168.2.3	0x51e7	No error (0)	kit.fontaw esome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 20:56:26.287740946 CET	8.8.8.8	192.168.2.3	0xa837	No error (0)	cdnjs.clou dflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Feb 22, 2021 20:56:26.287740946 CET	8.8.8.8	192.168.2.3	0xa837	No error (0)	cdnjs.clou dflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Feb 22, 2021 20:56:26.293267965 CET	8.8.8.8	192.168.2.3	0x71c2	No error (0)	maxcdn.boo tstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 20:56:26.299892902 CET	8.8.8.8	192.168.2.3	0x322a	No error (0)	stackpath. bootstrapc dn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 20:56:26.703097105 CET	8.8.8.8	192.168.2.3	0x4146	No error (0)	ka-f.fonta wesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 20:56:42.940218925 CET	8.8.8.8	192.168.2.3	0xe83f	No error (0)	www.politi kesgeuseis.gr		35.214.201.112	A (IP address)	IN (0x0001)

HTTPS Packets

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

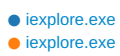
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 22, 2021 20:56:24.224509001 CET	173.237.190.111	443	192.168.2.3	49716	CN=webmail.architectchintanvirani.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Dec 28 03:49:34 CET 2020	Sun Mar 28 04:49:34 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		
Feb 22, 2021 20:56:24.224828005 CET	173.237.190.111	443	192.168.2.3	49715	CN=webmail.architectchintanvirani.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.	Mon Dec 28 03:49:34 CET 2020	Sun Mar 28 04:49:34 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		
Feb 22, 2021 20:56:25.262758017 CET	104.129.25.9	443	192.168.2.3	49718	CN=openplaywcowuk.gb.net 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.	Thu Feb 18 21:51:07 CET 2021	Wed May 19 22:51:07 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		
Feb 22, 2021 20:56:25.264322042 CET	104.129.25.9	443	192.168.2.3	49719	CN=openplaywcowuk.gb.net 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.	Thu Feb 18 21:51:07 CET 2021	Wed May 19 22:51:07 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		
Feb 22, 2021 20:56:26.465806007 CET	104.16.19.94	443	192.168.2.3	49730	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020	Thu Oct 21 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
							Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 22, 2021 20:56:26.468543053 CET	104.16.19.94	443	192.168.2.3	49731	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Feb 22, 2021 20:56:43.048461914 CET	35.214.201.112	443	192.168.2.3	49748	CN=politikesgeuseis.gr CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Jan 05 10:56:34 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Mon Apr 05 11:56:34 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 22, 2021 20:56:43.056911945 CET	35.214.201.112	443	192.168.2.3	49749	CN=politikesgeuseis.gr CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Jan 05 10:56:34 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Mon Apr 05 11:56:34 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 2024 Parent PID: 792

General

Start time:	20:56:22
Start date:	22/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff783160000
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: 752 Parent PID: 2024

General

Start time:	20:56:22
Start date:	22/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2024 CREDAT:17410 /prefetch:2
Imagebase:	0x10f0000
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