ID: 345132
Cookbook: browseurl.jbs
Time: 18:37:06
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report
http://mCFTbkD.deliberh.store/@20@40@#apeterson@ariasolutions.com 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Dropped Files 4
Sigma Overview 4
Signature Overview 4
Phishing: 5
Compliance: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 9
General Information 9
Simulations 9
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 15
No static file info 15
Network Behavior 15
Network Port Distribution 15
TCP Packets 16
UDP Packets 17
DNS Queries 18
DNS Answers 19
HTTP Request Dependency Graph 19
HTTP Packets 19
HTTPS Packets 19
Code Manipulations 20

Statistics 20
Behavior 20
System Behavior 20
Analysis Process: iexplore.exe PID: 6904 Parent PID: 800 20
General 20
File Activities 21
Registry Activities 21
Analysis Process: iexplore.exe PID: 6956 Parent PID: 6904 21
General 21
File Activities 21
Registry Activities 21
Disassembly 22

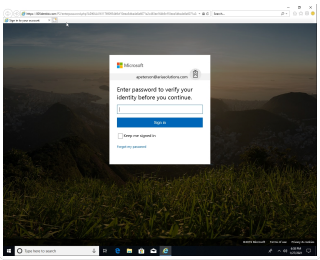
Analysis Report http://mCFTbkD.deliberh.store/@20@40…

Overview

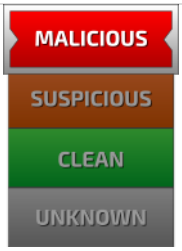
General Information

Sample URL:	http://mCFTbkD.deliberh.store/@20@40@#apeterson@ariasolutions.com
Analysis ID:	345132

Most interesting Screenshot:



Detection



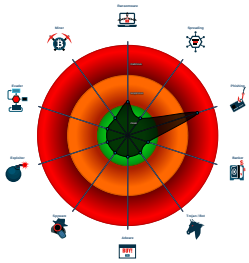
HTMLPhisher

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

Signatures

- Yara detected HtmlPhish_10
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- Invalid 'forgot password' link found
- Invalid T&C link found
- Suspicious form URL found
- URL contains potential PII (phishing…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6904 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6956 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6904 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

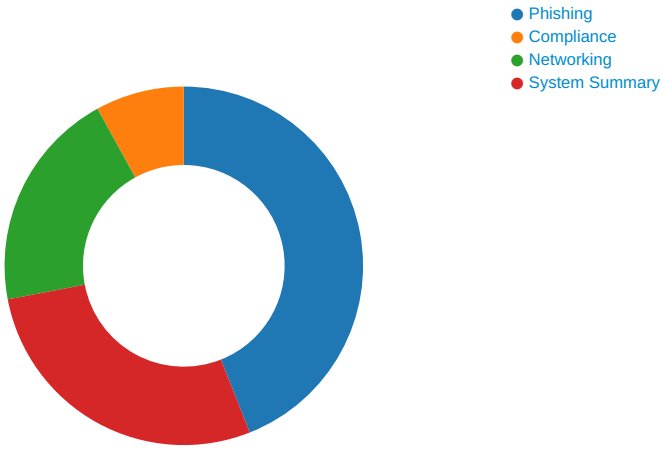
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\enterpassword[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

Phishing:

Yara detected HtmlPhish_10

Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

Compliance:

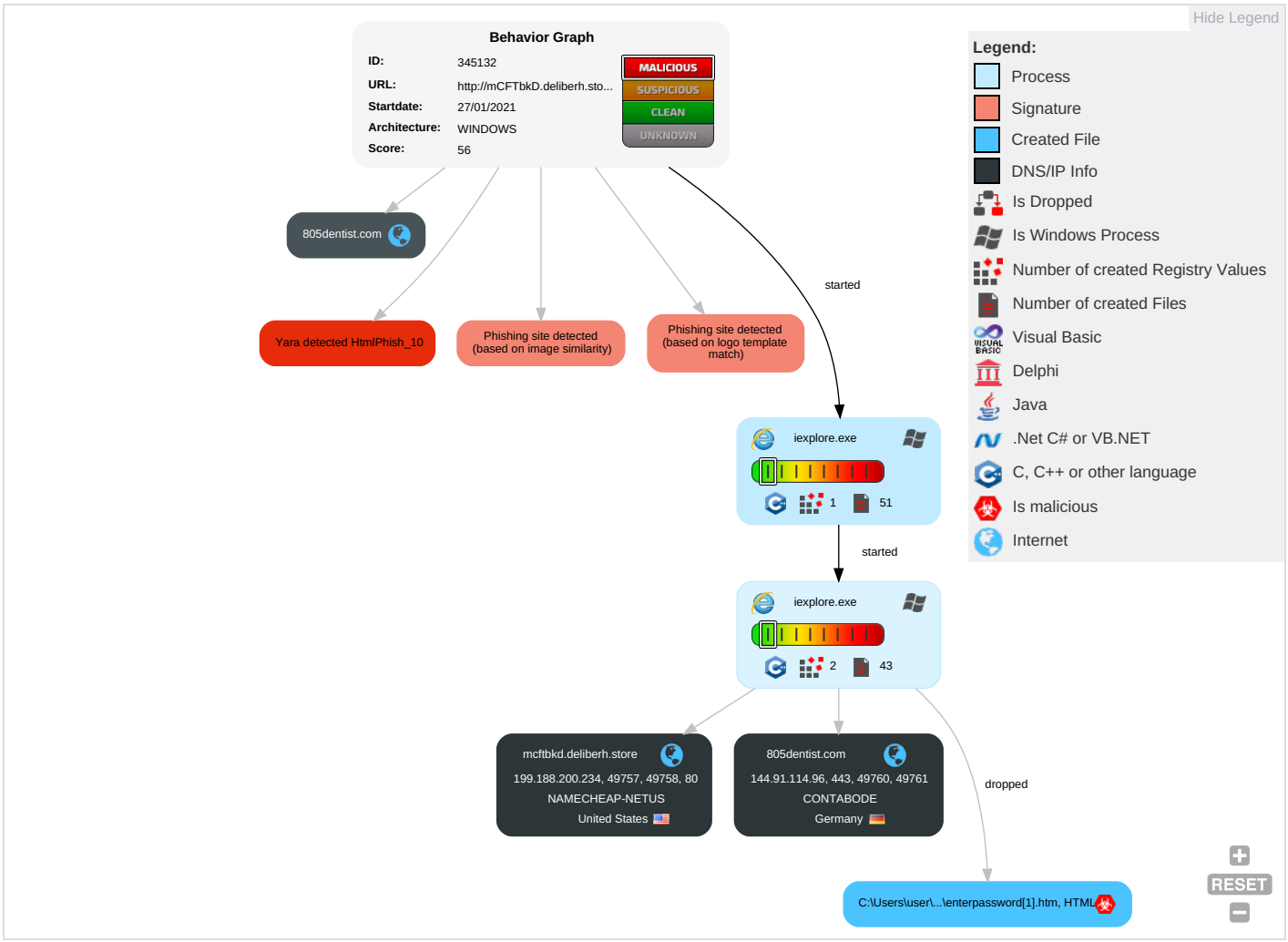
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
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 Partit
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 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carri Billin Fraud

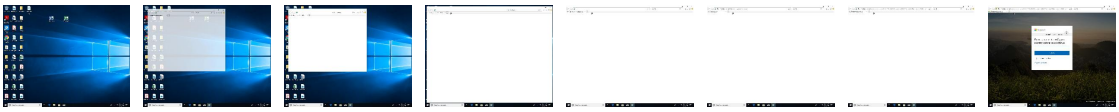
Behavior Graph

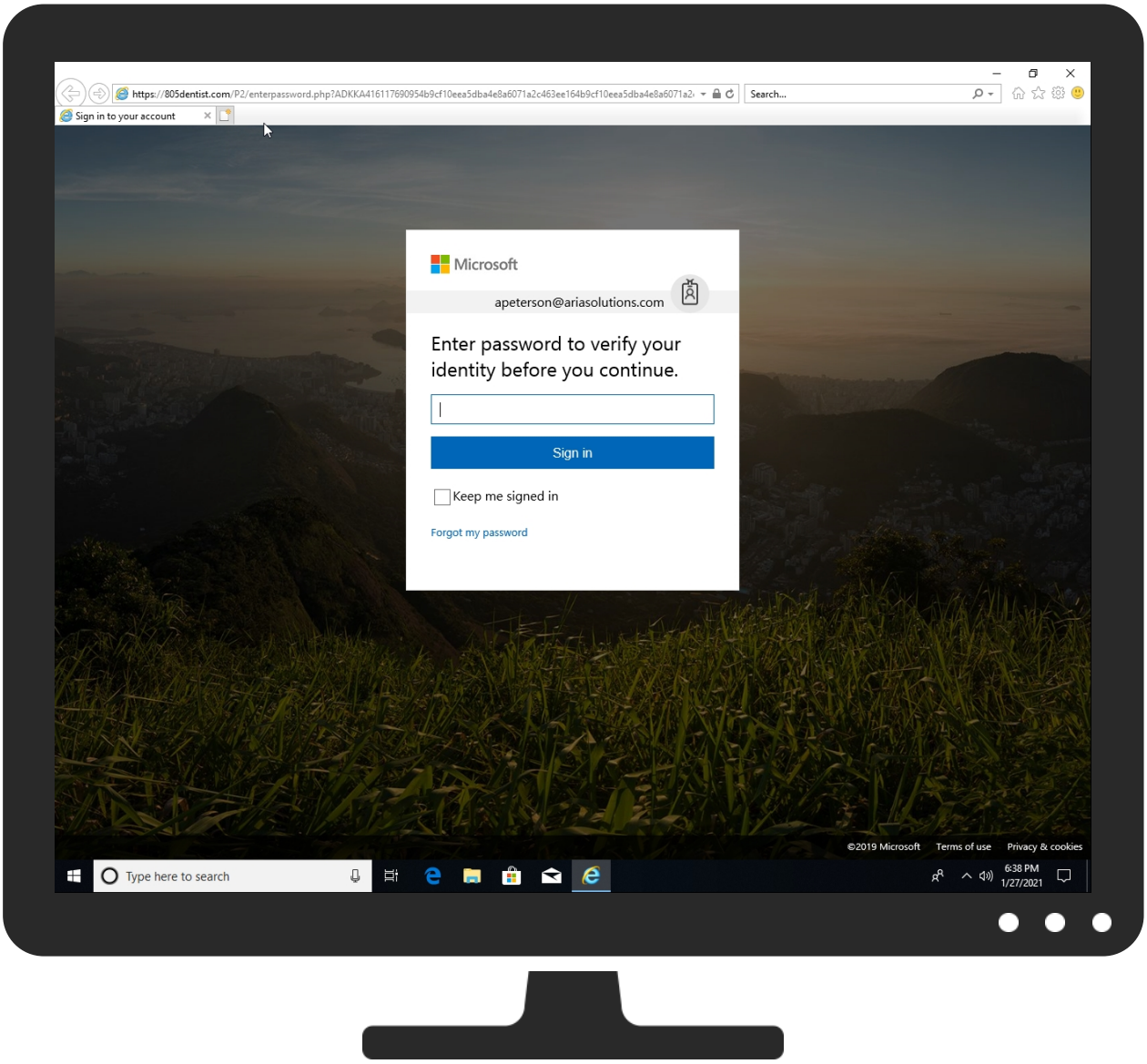


Screenshots

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://mCFTbkD.deliberh.store/@20@40@#apeterson@ariasolutions.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
805dentist.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://805dentist.com/P1/#apeterson	0%	Avira URL Cloud	safe	
http://https://805dentist.com/P2/?email=	0%	Avira URL Cloud	safe	
http://mcftbkd.deliberh.store/@20@40@	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://805dentist.com/P1/	0%	Avira URL Cloud	safe	
http://https://805dentist.com/P2/enterpassword.php?ADKKA416117690954b9cf10eea5dba4e8a6071a2c463ee164b9cf10e	0%	Avira URL Cloud	safe	
http://https://805dentist.com/P2/images/favicon.png%	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
805dentist.com	144.91.114.96	true	false	• 0%, Virustotal, Browse	unknown
mcftbkd.deliberh.store	199.188.200.234	true	false		unknown

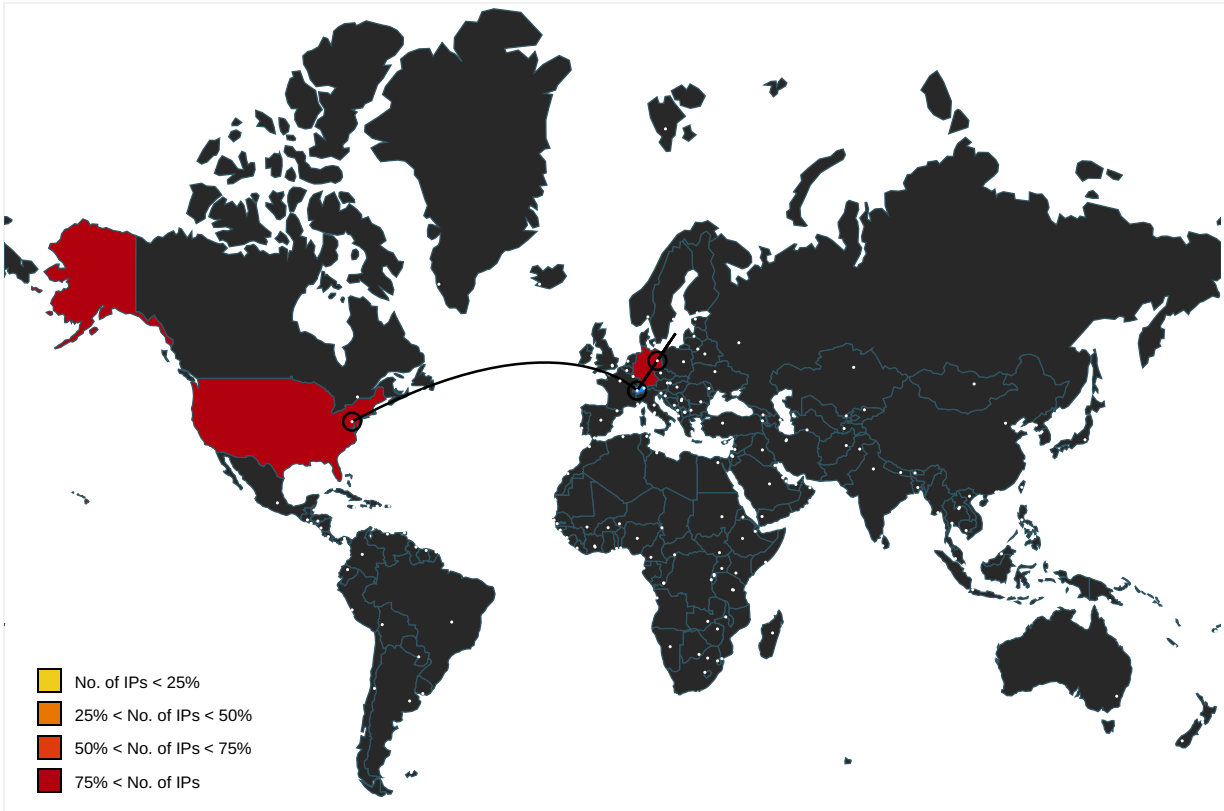
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://mcftbkd.deliberh.store/@20@40@	false	• Avira URL Cloud: safe	unknown
http://https://805dentist.com/P2/enterpassword.php?ADKKA416117690954b9cf10eea5dba4e8a6071a2c463ee164b9cf10eea5dba4e8a6071a2c463ee164b9cf10eea5dba4e8a6071a2c463ee164b9cf10eea5dba4e8a6071a2c463ee164b9cf10eea5dba4e8a6071a2c463ee16&email=apeterson@ariasolutions.com&error=	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://805dentist.com/P1/#apeterson	{61EF5F7C-60C6-11EB-90EB-ECF4BBEA1588}.dat.1.dr, ~DF31A818EA6B2EEE11.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://805dentist.com/P2/?email=	P1[1].htm0.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://805dentist.com/P1/	{61EF5F7C-60C6-11EB-90EB-ECF4BBEA1588}.dat.1.dr, P1[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://805dentist.com/P2/enterpassword.php?ADKKA416117690954b9cf10eea5dba4e8a6071a2c463ee164b9cf10e	{61EF5F7C-60C6-11EB-90EB-ECF4BBEA1588}.dat.1.dr, ~DF31A818EA6B2EEE11.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://805dentist.com/P2/images/favicon.png%	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
199.188.200.234	unknown	United States		22612	NAMECHEAP-NETUS	false
144.91.114.96	unknown	Germany		51167	CONTABODE	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345132
Start date:	27.01.2021
Start time:	18:37:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://mCFTbkD.deliberh.store/@20@40@#apeterson@ariasolutions.com
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.phis.win@3/16@3/2
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.108.39.131, 51.11.168.160, 95.101.22.216, 95.101.22.224, 152.199.19.161, 52.155.217.156 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, ie9comview.vo.msecnd.net, displaycatalog.md.mp.microsoft.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus17.cloudapp.net, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, cs9.wpc.v0cdn.net

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.{61EF5F7A-60C6-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.85387924625156
Encrypted:	false
SSDEEP:	192:r9Z+ZX2H9WQtzifG8uzM/2B6wDksf78PjX:rTqGHU0U/2Bz0
MD5:	09865E1CE569B5E77B2004A1F2CBB587
SHA1:	7CCBDE1D6E6274F231A0BD0E08E4512FBF68782C
SHA-256:	003C7E1D0BB3BA481AB3261C7C62C7695B64E6F23A86ED868B409D87D7303B1E
SHA-512:	B034C25ABDEC2C29962D971D3C8F9142A338B0F8844BBF807602F1C792F5B0F923D6B97317248FF416CF060A2AFF00CBACA2212C5807859CFFF4A431D2A4200
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\{61EF5F7C-60C6-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	32818
Entropy (8bit):	2.123578254057809
Encrypted:	false
SSDEEP:	768:XQiRRRR0RRMRRRR9RRRRqRRRRMRRRRlRRRRO:X9RRRR0RRMRRRR9RRRRqRRRRMRRRRlRk
MD5:	7F51E0E9E28401AAA4DEE3BF781CBA10
SHA1:	A8551795ED1E81C714B786645FC1020B90892F2E
SHA-256:	FD3579137A7600C3B3E1ADF08ADF9ADBE424ACE4B4D0AF11D09E51B768C300F3

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{61EF5F7C-60C6-11EB-90EB-ECF4BBEA1588}.dat	
SHA-512:	501504A366E3F26227B8702E2B3E11AB037EAE4D3621CF31522F2E7559D12DB0837C4AE733FE994E3CDC94D5584D4880E4F7DEF487724EDDB49D35CF51AD8D5
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\{6C1FA9EE-60C6-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5654465043801657
Encrypted:	false
SSDEEP:	48:Iw4GcprYGwpaZG4pQlGrapbSkrGQpKgG7HpRKsTGIpG:rMZAQ76VBSkFA7TK4A
MD5:	F46BD328788BCEA074C08C74CE42DF30
SHA1:	CA17B2EB2EDA253F68C9D420159A36CDD4090C19
SHA-256:	74043507A8CD52FE20D12475512398363D4E6B79C7F07DAFA740756F1ED42FE1
SHA-512:	0B73BD05AA958995D2EC8F4FF7DEA6197F33095DF3DBCBD56479AD0647C4865DFA7BA8C4EC0AFDD90309887DB02BF204072247127BB768A0D75153B733E97F5
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	3235
Entropy (8bit):	4.380571568888247
Encrypted:	false
SSDEEP:	24:/nSwtZEOxh5aNbyy007N7N7NZNZNAeNAeNaNaNaN8N855j7unR9Kev6HpNS5DXkc:/jgPRIYgASIICjKz
MD5:	F64C85AA0EC541E0FF41F36095F2930C
SHA1:	5A261F66A5537BCF12426ADBADE34B9DA6600A6C
SHA-256:	A432109521DCE765A67FAD1D2B1CE36AA8F75CB54BC21C8C4A88EE227299E8C9
SHA-512:	A195223E5C1D129C3D837CAA62EF8AC54DF0D6CF486B48953ECDEC01C9C41FC77756EC7020307DCAE9E645AD75A03DC3E4A2B1ED356A5BC83AC48CAF5739 6C
Malicious:	false
Reputation:	low
Preview:	,.h.t.t.p.s.:././.8.0.5.d.e.n.t.i.s.t...c.o.m./.P.2./.i.m.a.g.e.s./.f.a.v.i.c.o.n...p.n.g.%....PNG.....IHDR.....#....IDATx...?kdU.....5....b...hg./@.;.;_./f..K.+...rQ...-.....''..Y.&9 .y.0....?>w2.....K=;.../.]...../}?...N]W....o...g?,...u.I...Z.....RWOS....I.....ny...$.X.....@... .....@... .....@....@... .....@... .....@... .....F.. .....@... ....@... .....@... .....@... .....@... .....@... .....@... .....@... .....@... .....@... .....@... .....@... .....@... .....@... .....@... .....@.....@... .....@... .....@.....@... .....@... .....@... .....@... .....@.....@... .....@... .....@... .....@... .....@... ....@... .....@... .....@... ....@... .....@... .....@... ....@... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\P1[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	234
Entropy (8bit):	5.098938006827302
Encrypted:	false
SSDEEP:	3:PlyPhxn0+7/y9xwv7clXqy5AEtZ6UzUbX1XqSMuR0Lk3XmycXRyUEZcKBcD:pn0+Dy9xwol6hEr6VX16hu9nPT+KqD
MD5:	0E9F34A5E2B30F8B1CE2A5BD82D3C7E6
SHA1:	A1470A2ABC7661340B6130E332E6F0D69988DDB6
SHA-256:	FAE16E8F5191454EBAC096BDD26FB8502CE5D79FB7294BF6BC39B466055DB898
SHA-512:	34251D70748C71E23CA3628FB6B05BAAC9DE82DC6338DC8A4E56129B977EDB3DDB3A8598A0B3B5502C8FC1DEA8BA68A8C0756006B692E810F952C3B7CD630E C3
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\2WF3MMUU\jquery[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	95790
Entropy (8bit):	5.394132126458497
Encrypted:	false
SSDEEP:	1536:EPEkjP+iADIOr/NEe876nmBu3HvF38sEeL8FoqqhJ7SerN5wVI+xcBpPv7E+nzmN:bNMzqhJvN32cBd7M6Whca98Hr4
MD5:	4DC834D16A0D219D5C2B8A5B814569E4
SHA1:	4FBE0563917D6F6289E4E1B4A0A8758E4E43BDA9
SHA-256:	91222F96F34735EBC88DF208017E54D4329B9202E3E52367FB8B149698A1A5EF
SHA-512:	6FBEC4785A21520FA623D1A151C6C8B64BAA1321AC6918A127BCFC22E49EC2E3BCD161AF9C237BD5C70BC4046EB12CF434563F86CBDC9876EB67FB2DEA8704B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://805dentist.com/P2/js/jquery.js
Preview:	/*! jQuery v1.11.1 | (c) 2005, 2014 jQuery Foundation, Inc. | 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=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k={},l="1.11.1",m=function(a,b){return new m.fn.init(a,b)},n=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,o=/^-ms-/,p=/-([\da-z])/gi,q=function(a,b){return b.toUpperCase()};m.fn=m.prototype={jquery:l,constructor:m,selector:"",length:0,toArray:function(){return d.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var b=m.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a,b){return m.each(this,a,b)},map:function(a){return this.pushStack(m.map(this,function(b,c){re

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ms-logo-v2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 107x23, frames 3
Category:	downloaded
Size (bytes):	2797
Entropy (8bit):	7.505606447654921
Encrypted:	false
SSDEEP:	48:ay/EvnLPfuB5eJ3UKfOZisxPBY3yg3Mu/dDuXeYmDwuFbaAEj4QF8Ur5OMA:5k7urt0OBXYig3MfXeYxVD9fw
MD5:	5EC86907C1AC5EF3E117723998FEB8BE
SHA1:	5DAA2FEA5A34B0479A33698FC875F9F6C0581FD2
SHA-256:	BC2B16B51738B77D94ED7591AD1033FA804297CA9FAAA35222AA65773F749164
SHA-512:	AC052ED698BC59B14694C6A47979D20819658620896831E9A538C33AA0083659F2926773FFC3082C9965736C7C6EF11DACCBA8DD3B3C427B535EE2B88BA435E5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://805dentist.com/P2/images/ms-logo-v2.jpg
Preview:	......Exif..II*.....Ducky.....P.....zhttp://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.5-c021 79.154911, 2013/10/29-11:47:16 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:41705e1d-4a9a-1f43-8b65-c2b849c8cb4b" xmpMM:DocumentID="xmp.did:0E95A8B5216911E4B0C2C542DFA6230D" xmpMM:InstanceID="xmp.iid:0E95A8B4216911E4B0C2C542DFA6230D" xmp:CreatorTool="Adobe Photoshop CC (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:08ef3156-8bdf-8743-b5ba-46ec26c23b1b" stRef:documentID="xmp.did:41705e1d-4a9a-1f43-8b65-c2b849c8cb4b"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\0[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=7, xresolution=98, yresolution=106, resolutionunit=2, software=paint.net 4.0.13], baseline, precision 8, 1920x1080, frames 3
Category:	downloaded
Size (bytes):	298105
Entropy (8bit):	7.973045385700538
Encrypted:	false
SSDEEP:	6144:lUKZtJcr0nbPYZLCKZWbzLv6yTqMatTFuiaAQinJZB4zJZV+odViAagEHbSmXk:ncUgZWFbzzratOAQ2zB4znV+oPaBHPXk
MD5:	F5A9A9531B8F4BCC86EABB19472D15D5
SHA1:	0AAC0B09708622C679768AA62B11D95F0E8388DE
SHA-256:	62FAAB60433070E2EA52C235F0F18DB228759F2A08BB6F9E5711630DF8321214
SHA-512:	ED895FD0B400EC5362DFFC660492C477C9B5F4FE7E61EA65BC9D3FEE98402E132D719C8B05562F8EFE7C2D2BF4B1B825DDB07A2B37FD3AC1A6C47A24989BDBE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://805dentist.com/P2/images/0.jpg
Preview:	......JFIF.....``.....Exif..MM.*.....b.....j.(.....1.....rQ.....Q.....Q.....`.....`....paint.net 4.0.13.....C.....$ &%# #"(-90(*6+" #2D26;=@@@&0FKE>J9?@=...C.....=)#)=====.....8...."..... .!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w. .....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....8..)h.....$b.&.(.# ..B2jF.*.....QE1....i...A...P..1KJ(..R.iM.f.....!h...(...(...)h...(...Q.Z1@.....u.P0..Q@..1K..J).....h..K.P)i....J...h.1JE(L....H.....p.Zz...4.>...z.O....B.p.....(../qR.....G.....[.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\enterpassword[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	1821
Entropy (8bit):	4.896857014817123
Encrypted:	false
SSDEEP:	24:4WYePOuNYPpmzpwzicVvFGZhXqUsOotgivJPPPPCU+TRk2NENuBgVuygACHaeQKg:4tu6Ppm9wzDGZhADtg02a1P0xfkhD3
MD5:	0FDAF2CFB0BDE0FFF1B7DFB661FCC1BA
SHA1:	F7FD8712F9D60892A8AF7B6E284D3F5456607539
SHA-256:	74C2F12A627BCE727CF66380976C2BC1EB65C0818A63F20EB971C188B9F4D29A
SHA-512:	4963B0636D31D7BDA3518822AEB108F793764B6242CA02E4E93B0DE3CBA6D2B310B7507A78185AC0C6A063BCB17A750D4EC4AC03DFADF5DED0BCF9B8334EA D0B
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\enterpassword[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://805dentist.com/P2/enterpassword.php? ADKKA416117690954b9cf10eea5dba4e8a6071a2c463ee164b9cf10eea5dba4e8a6071a2c463ee164b9cf10eea5dba4e8a6071a2c463ee164b9cf10eea5dba4e8a6071a2c4 ee164b9cf10eea5dba4e8a6071a2c463ee16&email=apeterson@ariasolutions.com&error=
Preview:	.<!DOCTYPE html>.<html>.<head>..<title>Sign in to your account</title>..<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, minimum-scale=1.0, user-scalable=no">...<link rel="shortcut icon" type="icon" href="images/favicon.png">..<link rel="stylesheet" type="text/css" href="style.css">..<script type="text/javascript" src="js/jquery.js"></script>....</head>..<body>..<div class="overlay">...<div class="login-box">....<img src="images/ms-logo-v2.jpg" alt="logo">....<div id="identity" class="identity-banner">.....<div id="identity-name" class="identity">......apeterson@ariasolutions.com....</div>......<div class="profile-photo">......<img src="images/ms-logo-v1.svg" alt="logo">.....</div>....</div>.....<h2 id="title">Enter password to verify your identity before you continue.</h2>....<p id="message" class="message"></p>.....<div id="loader" class="loader hidden">.....<div class="circle"></div>.....<div class="circle"></div>.....<div class="circle"></div

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\favicon[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 640 x 640, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	3109
Entropy (8bit):	4.346081817367446
Encrypted:	false
SSDEEP:	24:oZEOxh5aNbyy007N7N7NZNZNAeNAeNaNaNaN8N855j7unR9Kev6HpNS5DXky0eR6:lPRIYgASlICjK8
MD5:	563829B27E0CDB44D229985A254C0672
SHA1:	B1EB6E4B62CA152CF05DDEA30EA6C3CB18AB5FA5
SHA-256:	FEB95D212B6B7595FF71BA5E54DF69B511ACBCD2831E9D7C8FE15CA3A2F011D9
SHA-512:	EF485A18FC23A30EF92B871792E9DCB684F70DEB5AC84FFDC7C0D7FAED2937594B22491CD665C2A5713B5BE3428E1333AD430A7693A3F1FACE150A459950FA 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://805dentist.com/P2/images/favicon.png
Preview:	.PNG........IHDR................#....IDATx...?kdU......5....b...hg./@.;.;_./f..K.+...rQ...-........"..Y.&9.y.0....?>w2..........K=;.../.].....}?...N]W....o...g?,...u.I...Z.......RWOS....I......ny...$. X.....@... ....@... ....@....@... ....@... ....@... ....F.. ....@... ....@... ....@... .....@... ....@... ....@... ....@... .....@... ....@... .. ..@... ....@... .....@... ....@... ....@... ....@... .....@... ....@... ....@... ....@.........@... ....@... ....@... ....@.........@... ....@... ....@... ....@.........@... ....@... ....@... ....@... ....@... ....@... ....@... ....@... ....@... ....@... ....@... ....@... ....@... ....@... ....@....@... ....@... ....@... ....@....@... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	6008
Entropy (8bit):	5.23590678922558
Encrypted:	false
SSDEEP:	96:xk5Xr5k9ZBDZU4OBY8kLtVO+uKYKekTktzplJVqm6NAZIOSBhLBL9LDDOp73xemL:xkDSOBPstVluKYHko1plJVqzNWWBhPDe
MD5:	6DF8DEAF769B76E5344701B8AF9E4446
SHA1:	EAB44FF0ABE0AFF7C77B98F4F08A030DFF20367A
SHA-256:	F3A3435DD1E14EA7EC192BE880BEFCE0C60C18A1DD6161F3A66CB82E9B358002
SHA-512:	E67363567875FE09B3218F5D54C05906055EACFB8DE5F3AA4C14CBCEA37877807888BA7A8E19FEAE91800120BA00B8C13B351DCCF67E1B8489B64219B1669C8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://805dentist.com/P2/style.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\style[1].css	
Preview:	* {...box-sizing: border-box;..}....body {...font-family: "Segoe UI Webfont",-apple-system,"Helvetica Neue","Lucida Grande","Roboto","Ebrima","Nirmala UI","Gadugi","Segoe Xbox Symbol","Segoe UI Symbol","Meiryo UI","Khmer UI","Tunga","Lao UI","Raavi","Iskoola Pota","Latha","Leelawadee","Microsoft YaHei UI","Microsoft JhengHei UI" ,"Malgun Gothic","Estrangelo Edessa","Microsoft Himalaya","Microsoft New Tai Lue","Microsoft PhagsPa","Microsoft Tai Le","Microsoft Yi Baiti","Mongolian Baiti","MV Boli", "Myanmar Text","Cambria Math";...margin: 0;...padding: 0;...width: 100%;...background-image: url('images/0.jpg');...background-repeat: no-repeat;...background-a ttachment: fixed;...background-position: center;...background-size: cover;...background-origin: border-box;..}.....overlay {...position: absolute;...width: 100%;...height: 100%;...background-color: rgba(0,0,0,0.55);..}....a { ...text-decoration: none; ...color: #0067b8;..}....a:hover { color: #005da6; }....footer {...display: block;...pos

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\P1[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	240
Entropy (8bit):	4.670546339585961
Encrypted:	false
SSDEEP:	3:qVvVF7XL//4Bbv//bl//kGFfHFa/YoK0O3FdF/qOkADFoHD4XRyz8lJqFqpCGXtc:qFVpsFkHFa/y7QmmHt8TqF0tFwHXBb
MD5:	A654D07186D877EC3754BF8056AB1CF5
SHA1:	DFD4CB62705FC4CADE0C2CBA18FBE611F73D4521
SHA-256:	3A0E4E3379476146CEA7D983AA7A37826DD3B31A1E7DE4D368B0D79B1A5C0C4D
SHA-512:	2F90A3576A708EAD653941871DB19C9BA8BE60F2717EA340A16015918E0063CA602F2A68E90CC9FF2E5F73DBD8361F976F32BE6300AF78882F5CBA5F21392AA0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://805dentist.com/P1/
Preview:	<html>. . <body>. . <script>. (function(){. var hash = window.location.hash; . window.location.href = "https://805dentist.com/P2/?email=" + hash.split('#')[1];. })();. </script>. </body>. .</html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\ms-logo-v1[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	756
Entropy (8bit):	4.879179443781471
Encrypted:	false
SSDEEP:	12:t4pb8WsQKvkBWSfYcW3ffBfYfomQO1a7aajR2F1hgWSnuCNSganii7v/NPujARqj:t4pb8WvKMTfY3ffBfYfomQO1eXjR2oug
MD5:	9DE70D1C5191D1852A0D5AAC28B44A6C
SHA1:	F4F64F5CBDBE6D1115C10A7F9CCB8828E6B67CAE
SHA-256:	5D3357BD875B7335ACE42E8EE3A64578E4253BED1A4E279109DE403EEDAE3A69
SHA-512:	CAC13FC2FE30E10772008F2AFF70FCA031EA9918E1F8C5C8B91CB9E79463383183406EFAADF89360DE3A08573FCDF2716C14DA6411E24B7E260B96AF84F0076
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://805dentist.com/P2/images/ms-logo-v1.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="48" height="48" viewBox="0 0 48 48"><title>assets</title><circle cx="24" cy="24" r="24" fill="#e6e6e6"/><path d=" M34,35V14a2.938,2.938,0,0,0-3-3H27V8l2-1L27.948,5.638,24,8,20.07,5.648,19,7l2,1v3H17a2.938,2.938,0,0,0-3,3V35a2.938,2.938,0,0,0,3,3H31A2.938,2.938,0,0 ,0,34,35Zm-3,1H17a.979.979,0,0,1-1-1V14a.979.979,0,0,1,1-1h6V10h2v3h6a.979.979,0,0,1,1,1V35A.979.979,0,0,1,31,36Z" fill="#404040"/><path d="M26.766,25 .42a4.432,4.432,0,1,0-5.533,0A6.237,6.237,0,0,0,17.765,31h1.653a4.582,4.582,0,1,1,9.165,0h1.653A6.237,6.237,0,0,0,26.766,25.42Zm-5.546-3.435A2.779,2.779,0,1,1,24,24.765,2.783,2.783,0,0,1,21.221,21.985Z" fill="#404040"/><rect x="21" y="14" width="6" height="2" rx="1" ry="1" fill="#404040"/></svg>

C:\Users\user\AppData\Local\Temp\~DF31A818EA6B2EEE11.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	42435
Entropy (8bit):	0.7962107722106021
Encrypted:	false
SSDEEP:	768:pZERRRRsRRRR9RRRRqRRRRMRRRRlRRRR:YRRRRsRRRR9RRRRqRRRRMRRRRlRRRR
MD5:	687093C978E94C055E84428AB5DA0108
SHA1:	E9A172087645DAC46D51D49BE2722DC21A2ED945
SHA-256:	9B6AB2EB0B8C094BBC56A9D175378DCFA566685B3C682E5D83BB700786D9679C
SHA-512:	D056235BE774710C46F12D251044A234BE982CCCFCA01102FF1E8495AD036B3A8DD7E4059FCC5DA5F5FA9A706CA0541C76F653E45E8031B736329BC282321F4
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF38E0EEEB062ED200.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.9223976001814125
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAr:kBqoxxJhHWSVSEab
MD5:	98F260E1774F99177DEDB55A41A12B9D
SHA1:	5231ADC5D8C929FE6054CC0C8C69F878A40B9019
SHA-256:	ED03F06C11BF62720C398334BA15BD47BA9B284CD60D3F37E977E238EED44184
SHA-512:	578CBB63616C02204208341FFCFD922723DB5C6D47699C187617704582BC35A341841F9EA241DE3B441FA704884C2AD5EEBDFB0895F0D00092282A7191FEB6FB
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(................... ....*%..H..M..{y..+.0...(................... ....

C:\Users\user\AppData\Local\Temp\~DF5E77D43CAB806751.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4783882869186001
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo0S9lo0C9lW0+gC9gBOGBNY9Y3:kBqoI0d0b0+gC9gBnBNY9Y3
MD5:	ADECCBF9EBABCF6D17EC5E11EBDE02CF
SHA1:	3BD650A57EBFB339EDA79DACEF5A3E25728B60F6
SHA-256:	C954EAE38567922F7F289A177DF4BCA8D5662922BE2B1EB3CF4C250CACFFE559
SHA-512:	DD87C360852535A75EDAABB7DE0B8BEC807956CB5CD1B12A16C1D008E33AE80E0E51E531DCCE84DB0A489488A39D79E8D1CEA47ADF93DA498CF1CA8497C4318
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: 85

- 53 (DNS)
- 443 (HTTPS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 18:37:54.973665953 CET	49757	80	192.168.2.4	199.188.200.234
Jan 27, 2021 18:37:54.974204063 CET	49758	80	192.168.2.4	199.188.200.234
Jan 27, 2021 18:37:55.175355911 CET	80	49757	199.188.200.234	192.168.2.4
Jan 27, 2021 18:37:55.175538063 CET	49757	80	192.168.2.4	199.188.200.234
Jan 27, 2021 18:37:55.176752090 CET	49757	80	192.168.2.4	199.188.200.234
Jan 27, 2021 18:37:55.187473059 CET	80	49758	199.188.200.234	192.168.2.4
Jan 27, 2021 18:37:55.187726974 CET	49758	80	192.168.2.4	199.188.200.234
Jan 27, 2021 18:37:55.375144958 CET	80	49757	199.188.200.234	192.168.2.4
Jan 27, 2021 18:37:55.375284910 CET	49757	80	192.168.2.4	199.188.200.234
Jan 27, 2021 18:37:55.450690031 CET	49760	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:37:55.450891018 CET	49761	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:37:55.500104904 CET	443	49761	144.91.114.96	192.168.2.4
Jan 27, 2021 18:37:55.500302076 CET	49761	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:37:55.501333952 CET	443	49760	144.91.114.96	192.168.2.4
Jan 27, 2021 18:37:55.501441002 CET	49760	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:37:55.505760908 CET	49760	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:37:55.505985975 CET	49761	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:37:55.556067944 CET	443	49761	144.91.114.96	192.168.2.4
Jan 27, 2021 18:37:55.778474092 CET	49760	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:37:56.090991020 CET	49760	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:37:56.700481892 CET	49760	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:37:57.904088974 CET	49760	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:37:57.952142000 CET	443	49760	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:11.398135900 CET	80	49757	199.188.200.234	192.168.2.4
Jan 27, 2021 18:38:11.398212910 CET	49757	80	192.168.2.4	199.188.200.234
Jan 27, 2021 18:38:11.409804106 CET	80	49758	199.188.200.234	192.168.2.4
Jan 27, 2021 18:38:11.409905910 CET	49758	80	192.168.2.4	199.188.200.234
Jan 27, 2021 18:38:11.917848110 CET	443	49761	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:11.917906046 CET	443	49761	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:11.917937994 CET	443	49761	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:11.918047905 CET	49761	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:11.920433044 CET	49761	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:11.948215961 CET	49761	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:11.953733921 CET	49761	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:11.996229887 CET	443	49761	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:11.998430014 CET	443	49761	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:11.998660088 CET	49761	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:12.008332014 CET	443	49761	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:12.008470058 CET	49761	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:12.011785030 CET	49761	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:12.099229097 CET	443	49761	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:12.188260078 CET	443	49761	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:12.188438892 CET	49761	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:12.258158922 CET	49761	443	192.168.2.4	144.91.114.96

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 18:38:12.306221008 CET	443	49761	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:12.571988106 CET	443	49760	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:12.572041988 CET	443	49760	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:12.572079897 CET	443	49760	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:12.572190046 CET	49760	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:12.572256088 CET	49760	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:12.572263956 CET	49760	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:12.575531960 CET	49760	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:12.623300076 CET	443	49760	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:12.633863926 CET	443	49760	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:12.634016037 CET	49760	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:15.809264898 CET	443	49761	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:15.809418917 CET	49761	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:15.811264038 CET	49761	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:15.859088898 CET	443	49761	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:15.865184069 CET	443	49761	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:15.865258932 CET	443	49761	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:15.865289927 CET	443	49761	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:15.865369081 CET	49761	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:15.865392923 CET	49761	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:15.868129969 CET	49761	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:15.927565098 CET	443	49761	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:15.927629948 CET	443	49761	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:15.927686930 CET	49761	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:15.927731991 CET	49761	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:15.938385963 CET	49761	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:15.938797951 CET	49760	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:15.941214085 CET	49768	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:15.941667080 CET	49769	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:15.987131119 CET	443	49760	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:15.988251925 CET	443	49769	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:15.988392115 CET	49769	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:15.989002943 CET	49769	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:15.989228964 CET	443	49768	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:15.989315033 CET	49768	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:15.989835024 CET	49768	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:15.992995024 CET	443	49761	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:15.993038893 CET	443	49761	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:15.993088007 CET	443	49761	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:15.993127108 CET	49761	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:15.993146896 CET	443	49761	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:15.993158102 CET	49761	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:15.993216038 CET	49761	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:15.993298054 CET	443	49761	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:15.993365049 CET	49761	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:15.995676994 CET	49761	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:16.001635075 CET	443	49760	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:16.001678944 CET	443	49760	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:16.001717091 CET	443	49760	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:16.001754045 CET	443	49760	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:16.001806974 CET	49760	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:16.001859903 CET	49760	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:16.001892090 CET	443	49760	144.91.114.96	192.168.2.4
Jan 27, 2021 18:38:16.001948118 CET	49760	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:16.001957893 CET	49760	443	192.168.2.4	144.91.114.96
Jan 27, 2021 18:38:16.001970053 CET	443	49760	144.91.114.96	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 18:37:47.414639950 CET	56627	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:37:47.465464115 CET	53	56627	8.8.8.8	192.168.2.4
Jan 27, 2021 18:37:48.348714113 CET	56621	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:37:48.409184933 CET	53	56621	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 18:37:49.803196907 CET	63116	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:37:49.851485968 CET	53	63116	8.8.8.8	192.168.2.4
Jan 27, 2021 18:37:50.642349005 CET	64078	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:37:50.695664883 CET	53	64078	8.8.8.8	192.168.2.4
Jan 27, 2021 18:37:52.169003010 CET	64801	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:37:52.217149973 CET	53	64801	8.8.8.8	192.168.2.4
Jan 27, 2021 18:37:53.026693106 CET	61721	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:37:53.074733019 CET	53	61721	8.8.8.8	192.168.2.4
Jan 27, 2021 18:37:53.864176989 CET	51255	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:37:53.925131083 CET	53	51255	8.8.8.8	192.168.2.4
Jan 27, 2021 18:37:54.089807987 CET	61522	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:37:54.149607897 CET	53	61522	8.8.8.8	192.168.2.4
Jan 27, 2021 18:37:54.891634941 CET	52337	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:37:54.952373028 CET	53	52337	8.8.8.8	192.168.2.4
Jan 27, 2021 18:37:55.054204941 CET	55046	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:37:55.111296892 CET	53	55046	8.8.8.8	192.168.2.4
Jan 27, 2021 18:37:55.385083914 CET	49612	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:37:55.445764065 CET	53	49612	8.8.8.8	192.168.2.4
Jan 27, 2021 18:37:55.845717907 CET	49285	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:37:55.895231009 CET	53	49285	8.8.8.8	192.168.2.4
Jan 27, 2021 18:37:56.677674055 CET	50601	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:37:56.728645086 CET	53	50601	8.8.8.8	192.168.2.4
Jan 27, 2021 18:37:58.214683056 CET	60875	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:37:58.267287970 CET	53	60875	8.8.8.8	192.168.2.4
Jan 27, 2021 18:38:12.708167076 CET	56448	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:38:12.756041050 CET	53	56448	8.8.8.8	192.168.2.4
Jan 27, 2021 18:38:16.837155104 CET	59172	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:38:16.896380901 CET	53	59172	8.8.8.8	192.168.2.4
Jan 27, 2021 18:38:19.962781906 CET	62420	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:38:20.020576954 CET	53	62420	8.8.8.8	192.168.2.4
Jan 27, 2021 18:38:23.861102104 CET	60579	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:38:23.909125090 CET	53	60579	8.8.8.8	192.168.2.4
Jan 27, 2021 18:38:24.524993896 CET	50183	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:38:24.574363947 CET	53	50183	8.8.8.8	192.168.2.4
Jan 27, 2021 18:38:24.860738993 CET	60579	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:38:24.908797026 CET	53	60579	8.8.8.8	192.168.2.4
Jan 27, 2021 18:38:25.531028986 CET	50183	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:38:25.588444948 CET	53	50183	8.8.8.8	192.168.2.4
Jan 27, 2021 18:38:25.859710932 CET	60579	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:38:25.912952900 CET	53	60579	8.8.8.8	192.168.2.4
Jan 27, 2021 18:38:26.681912899 CET	50183	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:38:26.729790926 CET	53	50183	8.8.8.8	192.168.2.4
Jan 27, 2021 18:38:27.876405954 CET	60579	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:38:27.924341917 CET	53	60579	8.8.8.8	192.168.2.4
Jan 27, 2021 18:38:27.938117027 CET	61531	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:38:27.997210979 CET	53	61531	8.8.8.8	192.168.2.4
Jan 27, 2021 18:38:28.513940096 CET	49228	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:38:28.575679064 CET	53	49228	8.8.8.8	192.168.2.4
Jan 27, 2021 18:38:28.687568903 CET	50183	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:38:28.735930920 CET	53	50183	8.8.8.8	192.168.2.4
Jan 27, 2021 18:38:29.055041075 CET	59794	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:38:29.112772942 CET	53	59794	8.8.8.8	192.168.2.4
Jan 27, 2021 18:38:29.585122108 CET	55916	53	192.168.2.4	8.8.8.8
Jan 27, 2021 18:38:29.642155886 CET	53	55916	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 18:37:54.891634941 CET	192.168.2.4	8.8.8.8	0xf67d	Standard query (0)	mcftbkd.de liberh.store	A (IP address)	IN (0x0001)
Jan 27, 2021 18:37:55.385083914 CET	192.168.2.4	8.8.8.8	0xdc4a	Standard query (0)	805dentist.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:38:16.837155104 CET	192.168.2.4	8.8.8.8	0xa50b	Standard query (0)	805dentist.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 18:37:54.952373028 CET	8.8.8.8	192.168.2.4	0xf67d	No error (0)	mcftbkd.de liberh.store		199.188.200.234	A (IP address)	IN (0x0001)
Jan 27, 2021 18:37:55.445764065 CET	8.8.8.8	192.168.2.4	0xdc4a	No error (0)	805dentist.com		144.91.114.96	A (IP address)	IN (0x0001)
Jan 27, 2021 18:38:16.896380901 CET	8.8.8.8	192.168.2.4	0xa50b	No error (0)	805dentist.com		144.91.114.96	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- mcftbkd.deliberh.store

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49757	199.188.200.234	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 18:37:55.176752090 CET	96	OUT	GET /@20@40@ HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: mcftbkd.deliberh.store Connection: Keep-Alive
Jan 27, 2021 18:37:55.375144958 CET	101	IN	HTTP/1.1 302 Found Date: Wed, 27 Jan 2021 17:37:55 GMT Server: Apache Location: https://805dentist.com/P1 Content-Length: 209 Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 38 30 35 64 65 6e 74 69 73 74 2e 63 6f 6d 2f 50 31 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head> <body> Found The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	199.188.200.234	80	192.168.2.4	49758	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 18:38:11.409804106 CET	150	IN	HTTP/1.0 408 Request Time-out Cache-Control: no-cache Connection: close Content-Type: text/html Data Raw: 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 3c 68 31 3e 34 30 38 20 52 65 71 75 65 73 74 20 54 69 6d 65 2d 6f 75 74 3c 2f 68 31 3e 0a 59 6f 75 72 20 62 72 6f 77 73 65 72 20 64 69 64 6e 27 74 20 73 65 6e 64 20 61 20 63 6f 6d 70 6c 65 74 65 20 72 65 71 75 65 73 74 20 69 6e 20 74 69 6d 65 2e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><body> 408 Request Time-out Your browser didn't send a complete request in time.</body> </html>

HTTPS Packets

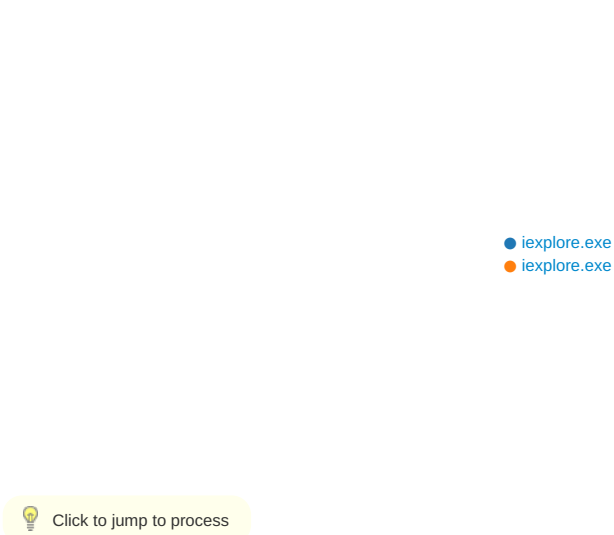
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 18:38:11.917906046 CET	144.91.114.96	443	192.168.2.4	49761	CN=805dentist.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 Jan 27 03:06:09 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Apr 27 04:06:09 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Jan 27, 2021 18:38:12.572041988 CET	144.91.114.96	443	192.168.2.4	49760	CN=805dentist.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 Jan 27 03:06:09 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Apr 27 04:06:09 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



System Behavior

Analysis Process: iexplore.exe PID: 6904 Parent PID: 800

General

Start time:	18:37:53
Start date:	27/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff63aa10000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 6956 Parent PID: 6904

General

Start time:	18:37:54
Start date:	27/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6904 CREDAT:17410 /prefetch:2
Imagebase:	0x1330000
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