ID: 426544
Cookbook: browseurl.jbs
Time: 01:26:05
Date: 29/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

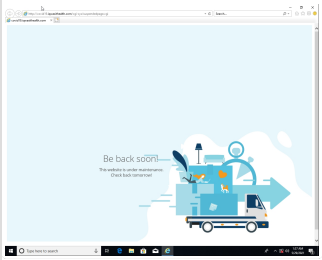
Analysis Report http://covid19.iqwasithealth.com/jillian-…

Overview

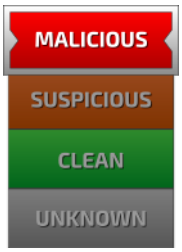
General Information

Sample URL:	http://covid19.iqwasithealth.com/jillian-ratke-iii/kathy_edler-43.zip
Analysis ID:	426544
Infos:	

Most interesting Screenshot:



Detection

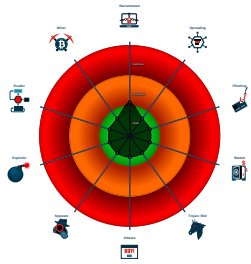


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Multi AV Scanner detection for doma…

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 5464 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4952 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5464 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

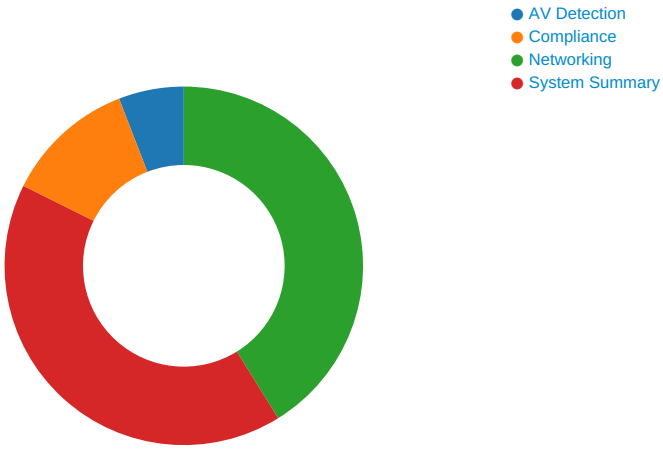
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

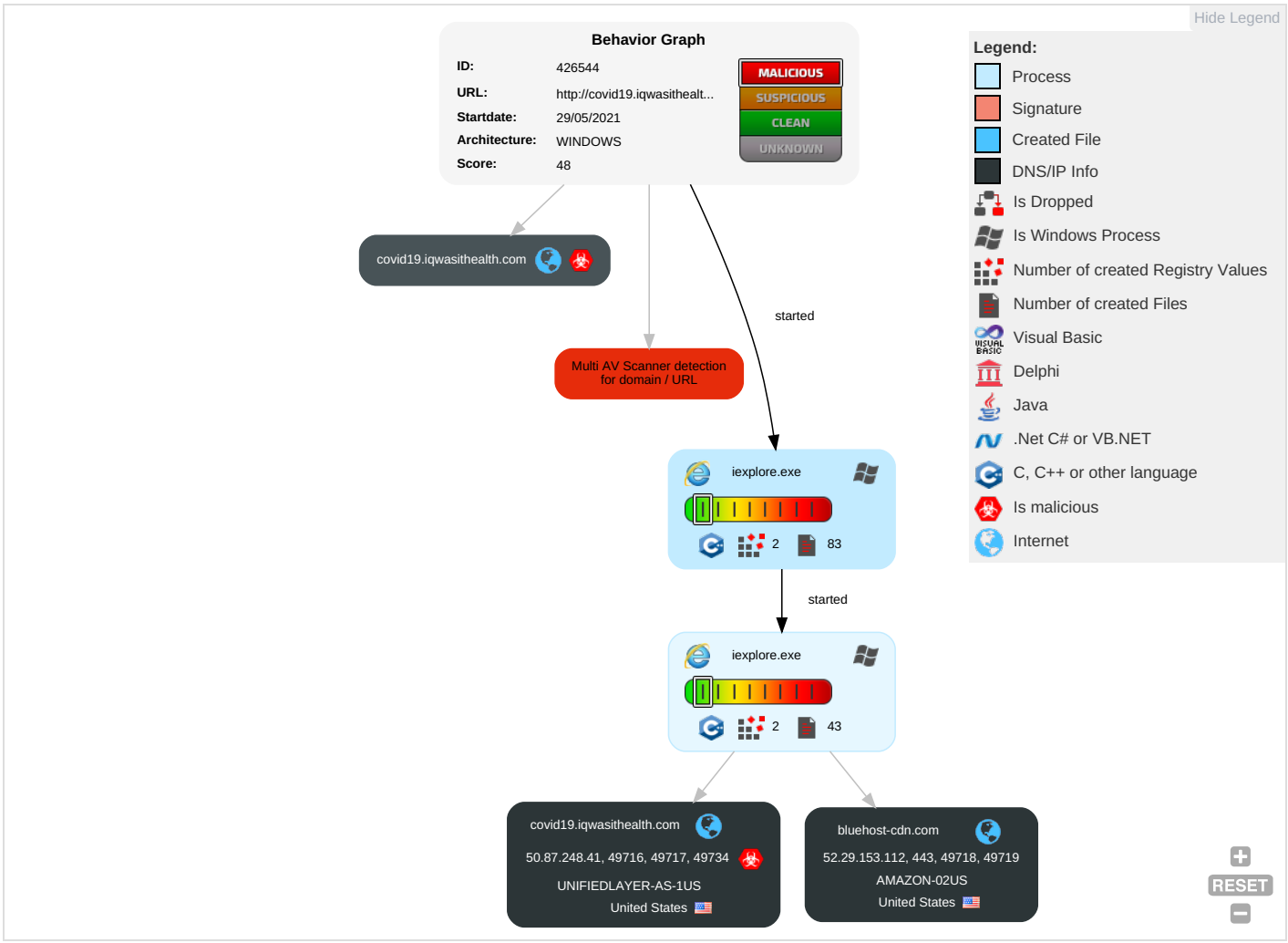
AV Detection:

Multi AV Scanner detection for domain / URL

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 3	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	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 4	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 2	SIM Card Swap		Carri Billing Fraud

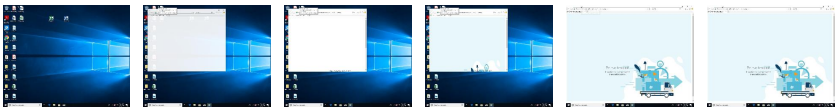
Behavior Graph

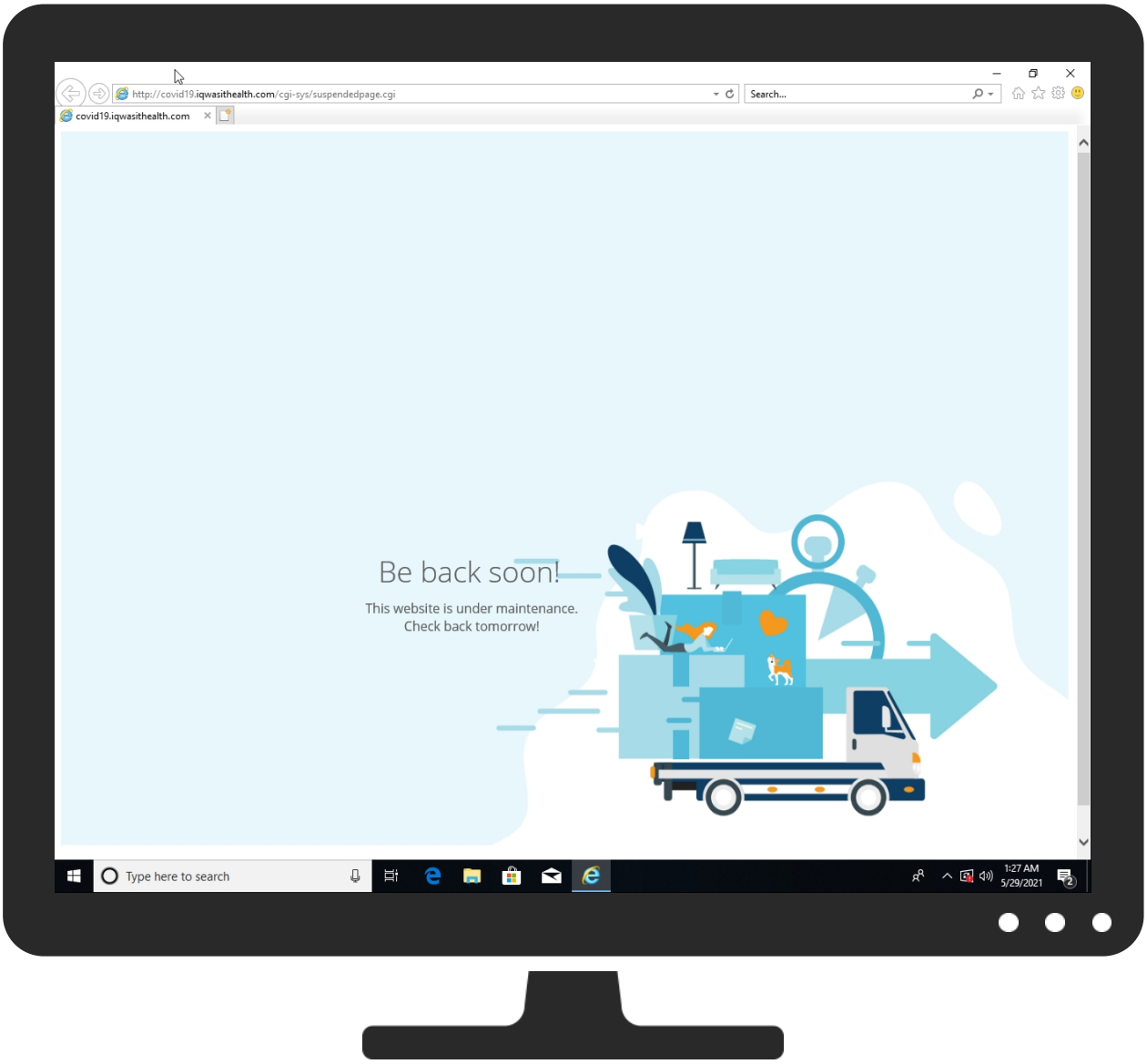


Screenshots

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://covid19.iqwasithealth.com/jillian-ratke-iii/kathy_edler-43.zip	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
covid19.iqwasithealth.com	6%	Virustotal		Browse
bluehost-cdn.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://bluehost-cdn.com/media/user/suspended_account/_bh/suspended.css	0%	Avira URL Cloud	safe	
http://covid19.iqwasithealth.com/cgi-sys/suspendedpage.cgiRoot	0%	Avira URL Cloud	safe	
http://covid19.iqwasithealth.com/favicon.ico	0%	Avira URL Cloud	safe	
http://bluehost-cdn.com/media/user/suspended_account/_bh/beback-soon.png	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
covid19.iqwasithealth.com	50.87.248.41	true	true	• 6%, Virustotal, Browse	unknown
bluehost-cdn.com	52.29.153.112	true	false	• 0%, Virustotal, Browse	unknown

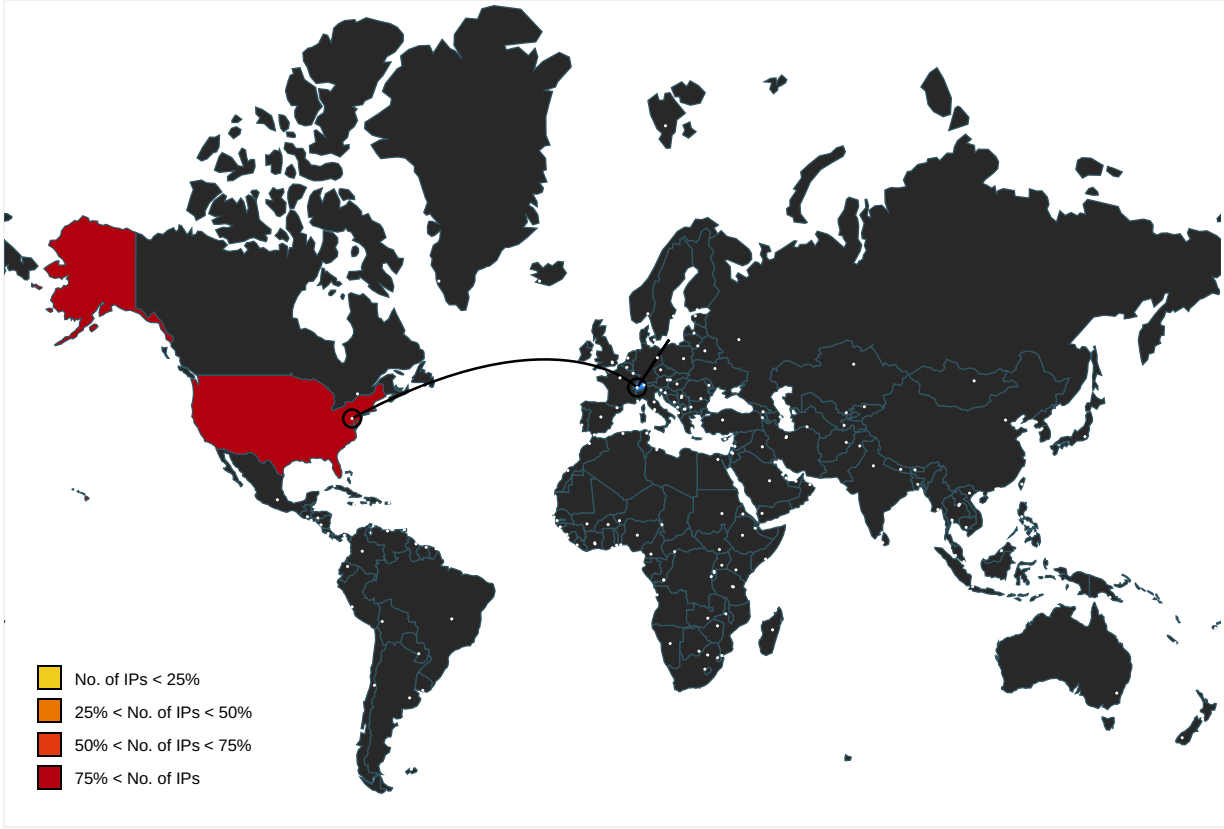
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://covid19.iqwasithealth.com/cgi-sys/suspendedpage.cgi	true		unknown
http://bluehost-cdn.com/media/user/suspended_account/_bh/suspended.css	false	• Avira URL Cloud: safe	unknown
http://covid19.iqwasithealth.com/favicon.ico	true	• Avira URL Cloud: safe	unknown
http://covid19.iqwasithealth.com/cgi-sys/suspendedpage.cgi	true		unknown
http://covid19.iqwasithealth.com/jillian-ratke-iii/kathy_edler-43.zip	true		unknown
http://bluehost-cdn.com/media/user/suspended_account/_bh/beback-soon.png	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.nytimes.com/	msapplication.xml3.2.dr	false		high
http://www.youtube.com/	msapplication.xml7.2.dr	false		high
http://www.wikipedia.com/	msapplication.xml6.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.com/	msapplication.xml.2.dr	false		high
http://www.live.com/	msapplication.xml2.2.dr	false		high
http://covid19.iqwasithealth.com/cgi-sys/suspendedpage.cgiRoot	{9C23E857-C057-11EB-90E4-ECF4BB862DED}.dat.2.dr	true	• Avira URL Cloud: safe	unknown
http://www.reddit.com/	msapplication.xml4.2.dr	false		high
http://www.twitter.com/	msapplication.xml5.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.29.153.112	bluehost-cdn.com	United States		16509	AMAZON-02US	false
50.87.248.41	covid19.iqwasithealth.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	426544
Start date:	29.05.2021
Start time:	01:26:05
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://covid19.iqwasithealth.com/jillian-ratke-iii/kathy_edler-43.zip
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.win@3/23@3/2

Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.43.139.144, 88.221.62.148, 172.217.22.234, 172.217.23.3, 20.82.210.154, 152.199.19.161, 104.79.90.110 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, fonts.googleapis.com, fs.microsoft.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus17.cloudapp.net, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.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.{9C23E855-C057-11EB-90E4-ECF4BB862DED}.dat

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{9C23E855-C057-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8560464800027794
Encrypted:	false
SSDEEP:	48:IwfGcpr6ZGwpLlG/ap8pGIpc4vGvnZpv4z3GoHqp94n2Go4Fpm4XGWRn94FGW7n1:r1ZyZB2bW4gt4zyf4nxFM4R4D4of4tMX
MD5:	A682E8FBC516F3E8AEFB0389A8CC8C3D
SHA1:	59B990E872ED7A9B489EFD51E290A7A4EDC6E45F
SHA-256:	3EF34468DAD4E6DA13FAA3AF867FA9C5D0814047FC0F7929C4AF8D1B07F767B9
SHA-512:	BADC5095BF478AA6E479DCF6F6F6D3CBDD8E9C28D6B049FEAEFBB3BF50E6B73C5FD223B4FFAC2BA5A247A80818D6163D92840C42AC4D425A91CF7A235AAA 67F
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\{9C23E857-C057-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24228
Entropy (8bit):	1.6435976024265642
Encrypted:	false
SSDEEP:	48:IwckGcpr2xZGwpaDkG4pQBWGrapbS6GQpBmGHHpcLTGUp8XGzYpmlxGopRnjDlzZ:rc4Z25QDU6BYBSCjl2lWVMZXAzeg
MD5:	4A8C8D697E3BF87DF25AC9A2BE4E06C7
SHA1:	425D4EEE76CA70E7F69978BE8185543221EB7EF5
SHA-256:	E063B1A4BDFA17AB163533865D548C236E0DBCBA3D076348D7AFA73FBBB42D2B
SHA-512:	AE4D45DFE18FC4DC3EEC50400DB227C982B6DEAF0A2FFF950610EE435E0389B74D324F1FFF673BB56982CDDFAE6570A6FA7860A403D9141B6AD56B7D4D8E9E 13
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\{9C23E858-C057-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5644094272038276
Encrypted:	false
SSDEEP:	48:IwxGcprcZGwpapG4pQVGrapbSXGQpKxG7HpRLTGIpG:rHZoQr6FBShAgThA
MD5:	FFEB765104CF7C6AE410EA4264DCDBAC
SHA1:	6EE453BC36BD44AD5111A4E6B76254F649A4881F
SHA-256:	E2D88BF46A93FFB6E301B769C5B4A5D195CB041E96E6AC4A9394F18CEE670AA4
SHA-512:	E73357F8B735705D10FE854ADB94D00E050F33F2F610A60A5929F4F5633DDB918A9199872B1958F19460355F5F74207ABC45D7520E2DF8A9E3528E57241DED46
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.159275399236635
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
SSDEEP:	12:TMHdNMNxOEiibnWimI002EtM3MHdNMNxOEiibnWimI00ObVbkEtMb:2d6NxO/ibSZHKd6NxO/ibSZ76b
MD5:	4E424A52E2D62B48485C69536FFD1F33
SHA1:	9F0F0C60E6D2E6AF73850A5CADCB7D53760F0038
SHA-256:	0A34190FD566E445D73856BFDD25D9B565BE21726C1EB3E22ED01E008894618F
SHA-512:	5F98C6B924F2094B205A2B8B3677CDD0F96CB96E34329C4E71E9A0A15A8C9FA961C9B8D51587349BB9DB13370BF6C7D4559FE05C615ACF0309525F5167F2D6B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x7299f579,0x01d75464</date><accdate>0x7299f579,0x01d75464</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x7299f579,0x01d75464</date><accdate>0x7299f579,0x01d75464</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.156140228019286
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2k7nWimI002EtM3MHdNMNxe2k7nWimI00Obkak6EtMb:2d6NxreSZHKd6NxreSZ7Aa7b
MD5:	C058190A5EC13A392F9E287DC7840B92
SHA1:	14B69A5832A20D7539E9776B3967DD3CF66E2519
SHA-256:	450B7C6E3291CB13F075541C519489F8DBDEE6C26288BC8262FC290CA1C907AB
SHA-512:	D8A6C3ECFD0834F781E6B444FE40C463FDE3A18360D7C6EA53F5B1C6F06C51B809B590B3856B1FA59BC8848E10E732026D78F46A391F5FC1C395602319B4E5F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x728ba75c,0x01d75464</date><accdate>0x728ba75c,0x01d75464</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x728ba75c,0x01d75464</date><accdate>0x728ba75c,0x01d75464</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.178691481683391
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLiibnWimI002EtM3MHdNMNxvLiibnWimI00ObmZEtMb:2d6NxvOibSZHKd6NxvOibSZ7mb
MD5:	BF3A96369C13EFE2094D6018AD31DB4D
SHA1:	42A94A4B55EBB4BED012781979D1AEDC697190A0
SHA-256:	CD467B4829A80AC1136E46F1A9BB69D626CFB80D3FBD45319E67CD26095FAA61
SHA-512:	34025EB332286ACEC9B6DAF88E3670097A1D7961C9FF2853F8EBB4DEAD3DAD6FA19F60765F2ED98FBD80729832B73B3F8947DFD4E4B01B6807116801DD6E088C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x7299f579,0x01d75464</date><accdate>0x7299f579,0x01d75464</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x7299f579,0x01d75464</date><accdate>0x7299f579,0x01d75464</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.174073617547099
Encrypted:	false
SSDEEP:	12:TMHdNMNxiU2L26nWimI002EtM3MHdNMNxiU2L26nWimI00Obd5EtMb:2d6Nxh2L26SZHKd6Nxh2L26SZ7Jjb
MD5:	CCDFD2F7A6FAB6D4BF77A25192F0F522
SHA1:	34AD5C14B8BA4D3CE9839116CAABFAE5171F6F4B
SHA-256:	6A017D01FB6624105DB865C78114D1EF973A2983B3F28C5DD7008902F74CB549

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
SHA-512:	13C5A5D8DCC3DB978D05FFCD1D4DD411F75F2E108504785AEA3A4ECDDFAD94FED1D2045C3555A18C8F6EB8B03B6F28572D446A8932EFC9F6CD597032279143 7
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x72979314,0x01d75464</date><acc date>0x72979314,0x01d75464</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x72979314,0x01d75464</date><accdate>0x7297 314,0x01d75464</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.194037885600458
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwiibnWimI002EtM3MHdNMNxhGwiibnWimI00Ob8K075EtMb:2d6NxQTibSZHKd6NxQTibSZ7YKajb
MD5:	CEB1F7A7A36F21EA1F20ED77EDBA4051
SHA1:	48F328756B60E9CC3C31459836DC345F8DBBFD6B
SHA-256:	BD6B48F71A89F44BF87554ADF393D2AC2F072351536C251ABA5CD50F4263E4DA
SHA-512:	DEB9DB60AC6EE430ADE3D259C99DCF6AE8A9D981516A3A018457C90956F3E913BBE07CAC3AE4ED841CC6B56BAD1DB482D2D617E4F27E268864ADB406DFC4 92E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x7299f579,0x01d75464</date>< accdate>0x7299f579,0x01d75464</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x7299f579,0x01d75464</date><accdate>0 x7299f579,0x01d75464</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.162744528526615
Encrypted:	false
SSDEEP:	12:TMHdNMNx0niibnWimI002EtM3MHdNMNx0niibnWimI00ObxEtMb:2d6Nx0iibSZHKd6Nx0iibSZ7nb
MD5:	A0814D40C3DCDA9A8A7B414964D56056
SHA1:	301875A09F5C540DAE68C8787D89181F910652A7
SHA-256:	40F19CB431710936D77359D9AA25BE2D49822D8BD35F5B66E4B45D3D65212E44
SHA-512:	DFFF600D23C24DD10A7F704774E958AAA1C8A003CD2DD7A51E9C951DA0DE3099F40051C97230EC18D5343A06676D7637F711732825FDD8A9046EAA9F530CFE9
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x7299f579,0x01d75464</date><a ccdate>0x7299f579,0x01d75464</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x7299f579,0x01d75464</date><accdate>0x7 299f579,0x01d75464</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin202591677780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.197860579184103
Encrypted:	false
SSDEEP:	12:TMHdNMNxxU2L26nWimI002EtM3MHdNMNxxU2L26nWimI00Ob6Kq5EtMb:2d6NxK2L26SZHKd6NxK2L26SZ7ob
MD5:	5C0B4D2F0808CC040B32B1FD4591017A
SHA1:	D314C7CC583C723D4C22CEA8C0DF5E9A8E98F0B7
SHA-256:	F1D70FC18C6CFB32A59073F0E72D58B67D32C8F02992BF9D9CBFE0607BFEE23D
SHA-512:	7DF16589CD943CABEC64867055115123B5F38B667D611033AE23D821FB37F08EDA184D9D0190B934CB4610ED9EAC0D4010351C034647C684545C0986E993777F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x72979314,0x01d75464</date><accdate>0x72979314,0x01d75464</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x72979314,0x01d75464</date><accdate>0x72979314,0x01d75464</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.160420881726496
Encrypted:	false
SSDEEP:	12:TMHdNMNxc4Z6nWimI002EtM3MHdNMNxc4Z6nWimI00ObVEtMb:2d6Nx2SZHKd6Nx2SZ7Db
MD5:	AE442E3D1D5525323CB30C634185E495
SHA1:	7B42401AE65644BE60591DED3C83870720C391A8
SHA-256:	4EE30FC9E76148569D0DADF3B3F44619D440E8E5FF377DC9C49427C40BCD6CCF
SHA-512:	27E61BE97AA49C95AEE49F219F2CB9252114E5EA3786A18E9FE87EA3D7E536F1C921FB1E16464C68308746FFC2D01178B057BFAB1FC12FE0EE5FAC418AA82DD3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x729530cf,0x01d75464</date><accdate>0x729530cf,0x01d75464</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x729530cf,0x01d75464</date><accdate>0x729530cf,0x01d75464</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.15915877689611
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnU2L26nWimI002EtM3MHdNMNxfnU2L26nWimI00Obe5EtMb:2d6NxM2L26SZHKd6NxM2L26SZ7ijb
MD5:	9BF133C1759AD6DF32A9CEF72172EB7D
SHA1:	2E439C560A663119390F3A43E8D511039CE60310
SHA-256:	47D006ADDBC47BE9189A3375CDB2D37861F9F4F80486D39D8927C9FBE8E6158B
SHA-512:	87E435F3820F2A34432E4834D3ADA9EE5B09EFBEF436AB810ACD711103B3CF6DB1FA7806D0691CA0203795B0CEC317F46F11FCC17A4E51EBA107C8581990EA34
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x72979314,0x01d75464</date><accdate>0x72979314,0x01d75464</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x72979314,0x01d75464</date><accdate>0x72979314,0x01d75464</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\beback-soon[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1430 x 982, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	43201
Entropy (8bit):	7.659124990561904
Encrypted:	false
SSDEEP:	768:LugxQTPvEE/wt7V88rsJDyE+w04UgOHX0voOdejIU0MKADQzR+Ra:LSDcewB5r8DyEs4XO30voOeZDU84
MD5:	495826852EE860B53716AEEDFCAD9F75
SHA1:	6FF9EEF566AA5BFE11749B37E16C1F24941633CC
SHA-256:	A9119A330A2C1F636051FC96E31AF730D7BD096D358D7AD1681AC3770630F4A8
SHA-512:	8A6DEE67E925081690D085DC789E7142F33F8C131323A3C067F46C0E2C913EF6651AC64EE61067C6E678FCBAF0FFA91F4BC6CE814F3050647D2736E63609A326
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bluehost-cdn.com/media/user/suspended_account/_bh/beback-soon.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\beback-soon[1].png	
Preview:	.PNG.....IHDR.....s..Q....IDATx...Q.. .....k.z.P...}.....'.....,..e.....2....b.....X.....@,.....X.....@,..... .....e.....2.....e.....2....b.....X.....@,.....X.....@,..... .....T.....e.....2....b.....X.....X.....@,..... .....e.....e.....2....b.....X.....X.....@,..... .....$.....e.....2....b.....b.....X.....@,..... ... .e.....2....b.....b.....X.....@,..... .S..... .....e.....2....b.....2....b.....X.....@,..... .....@,..... .....e.....2....b.....2....b.....X.....@,..... @,..... .....e.....2.....e.....2.....b.....X.....@,.....X.....@,..... .....e.....2.....e.....2.....b.....XN.....X.....@,..... .....e.....e.....2.....b.....X..... .....X.....@,..... .....e.....e.....2.....b.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\css2[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	410
Entropy (8bit):	5.090272386896636
Encrypted:	false
SSDEEP:	12:jFMO6ZGqtKspLtf1qFMO6ZRoMqtKspLtUxY:5MOYGaK/MOY7aKA
MD5:	2FA25E285A753FB92A157D62EBA152FF
SHA1:	E46518F1F513AFA95C5E7A446BA9E296AAB687F0
SHA-256:	CFA4432D8EBA96FA3CFE49E0F6EBD9AB197CDC18D50EBB8D019B33E958C34B44
SHA-512:	6CE97AA154849E1F2808F04059156F45341E1803D4243A5AF133B8F9287874DDE71AABA9FB379550F53540F6D444FFC5BACABEB210BBEA0C8473085B2B532F4E
Malicious:	false
Reputation:	low
IE Cache URL:	http://fonts.googleapis.com/css2?family=Open+Sans:wght@300;400&display=swap
Preview:	@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 300;. font-display: swap;. src: url(http://fonts.gstatic.com/s/opensans/v20/mem5YaGs126MiZpBA-UN_r8-Vg.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(http://fonts.gstatic.com/s/opensans/v20/mem8YaGs126MiZpBA-U1UQ.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\beback-soon[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	162
Entropy (8bit):	4.43530643106624
Encrypted:	false
SSDEEP:	3:qVoB3tUROGclXqyvXboAcMBXqWSZUXqXllVLLP61IwcWWGu:q43tISl6kXiMIWSU6Xll5LP8IpfGu
MD5:	4F8E702CC244EC5D4DE32740C0ECBD97
SHA1:	3ADB1F02D5B6054DE0046E367C1D687B6CDF7AFF
SHA-256:	9E17CB15DD75BBBD5DBB984EDA674863C3B10AB72613CF8A39A00C3E11A8492A
SHA-512:	21047FEA5269FEE75A2A187AA09316519E35068CB2F2F76CFAF371E5224445E9D5C98497BD76FB9608D2B73E9DAC1A3F5BFADFDC4623C479D53ECF93D81D3C F
Malicious:	false
Reputation:	low
Preview:	<html>..<head><title>301 Moved Permanently</title></head>..<body>.. 301 Moved Permanently ..<hr> nginx ..</body>..</html>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\suspended[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	162
Entropy (8bit):	4.43530643106624
Encrypted:	false
SSDEEP:	3:qVoB3tUROGclXqyvXboAcMBXqWSZUXqXllVLLP61IwcWWGu:q43tISl6kXiMIWSU6Xll5LP8IpfGu
MD5:	4F8E702CC244EC5D4DE32740C0ECBD97
SHA1:	3ADB1F02D5B6054DE0046E367C1D687B6CDF7AFF
SHA-256:	9E17CB15DD75BBBD5DBB984EDA674863C3B10AB72613CF8A39A00C3E11A8492A
SHA-512:	21047FEA5269FEE75A2A187AA09316519E35068CB2F2F76CFAF371E5224445E9D5C98497BD76FB9608D2B73E9DAC1A3F5BFADFDC4623C479D53ECF93D81D3C F
Malicious:	false
Reputation:	low
Preview:	<html>..<head><title>301 Moved Permanently</title></head>..<body>.. 301 Moved Permanently ..<hr> nginx ..</body>..</html>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\suspended[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\suspended[1].css	
Category:	downloaded
Size (bytes):	608
Entropy (8bit):	4.936107954795618
Encrypted:	false
SSDEEP:	12:DuLB/p+oEdwZuyG5QAIrIyxYM6ZR32vmMo5Q2PXPFMYw032vOXsw03en:SF6dquyGSAExYRGvfoSe/Ffw0GvOcw0W
MD5:	FCC0451FD57AE709762EFCCA96001902
SHA1:	D1B2F74C3CF5B11BE47E6A780FDF640A25F245A8
SHA-256:	62A3B1D143DB0EA140983CDF2A54D4B87973AAF409B6B4C8370595C80AE5AF9C
SHA-512:	9CB12D080D71B13BA091DAEE7B4FB1A9C058A9DB677610D68CA480FDB47D5E64AAA011E4E2426BC68EDC5852DCD97A69ACAA9050160A6AA6F8C9F70660E9FDB7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bluehost-cdn.com/media/user/suspended_account/_bh/suspended.css
Preview:	.suspend-photo {. background: transparent url('bh-beback-soon.png') no-repeat;. background: center;. width: 100%;. height: 880px;. opacity: 1;.}..be-back {. position: absolute;. font-size: 36px;. top: 496px;. left: 400px;. color: #5C5C5C;. opacity: 1;. font-weight: 200;. font-family: 'Open Sans', sans-serif;.}..website-moved {. position: absolute;. font-size: 16px;. text-align: center;. top: 569px;. left: 384px;. color: #5B5B5B;. font-family: 'Open Sans', sans-serif;.}..questions {. text-align: center;. color: #5B5B5B;. font-family: 'Open Sans', sans-serif;. font-size: 15px;.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\mem5YaGs126MiZpBA-UN_r8-Vg[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 57032, version 1.1
Category:	downloaded
Size (bytes):	57032
Entropy (8bit):	**7.992677920510295**
Encrypted:	**true**
SSDEEP:	1536:cyjs0/Ma1mbvuRVHFEVlHendxvHXdlgrSGZVm:ts09iur67YXvtlgrSGZVm
MD5:	9E55836C60E94AAD92DEE91796D5DCCB
SHA1:	086F64719F7B56B2ACA277B74D0561F40E49CFAB
SHA-256:	F90019961C130188453DEA8C8A1AA419DA9D414F62E75462980ACE71794D66D5
SHA-512:	04FD2FAFFE102FD270D290C8805E4B3E241DA9D34D7BC9411A9862A625CEF7B18BD21BF0CBBE733BE73D0EB786FF7306D294555351664CC8780B9AAFF008B64
Malicious:	false
Reputation:	low
IE Cache URL:	http://fonts.gstatic.com/s/opensans/v20/mem5YaGs126MiZpBA-UN_r8-Vg.woff
Preview:	wOFF.....~.....GDEF.....-....2.oGPOS.....GSUB.....>.u.4OS/2...x...^...`...cmap.....h.....cvt ...@...]....fpgm.....~a..gasp...<.....#glyf...L.....9.6...head.....6...6..F.hhea..... ...$....hmtx...(...l.....AOloca.....maxp...h... ... .E..name.....c?Jpost...t...<....Y...prep.....:..]x.c`d``.a..&.V .....$...../s..#s.s..#. ..x.U..n.@.D..Em.....q.....s...NH$.....t~f..fxy.....qDD..$`$.r.....?<.<b...N.....W.....a....L9.,"@$".[E....=B..'3....)O...".[=..W...R..j.m..(.6.....c..0...c.!F_.C.+S..x.c`fig.a`e``..j...(.../2.1..`b.ffcfeabby....A!...A.....ah..e.P``...c.g.....x.....1....Lj.ivk.m.m..j.m...W....w.1~.@ ....N..`/.P..C.....&.X..a/..3p9>B.b.Ll3....+.)!...p....P.N.i.....I:..R.4..k.|.....(?.$.@.K....A.X<....d.).-...2..*....."{..r.\..."YQ-i.VB+.U.fvP;...i.;.].m7Hp.-..VZ..4..0...qL....7...8....{..q.WG.....1.f.."

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\mem8YaGs126MiZpBA-U1UQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 55324, version 1.1
Category:	downloaded
Size (bytes):	55324
Entropy (8bit):	**7.99064619923168**
Encrypted:	**true**
SSDEEP:	1536:JjsyS1KN5BvtgX74JT3XeCuDfKQDpoKyT0756MILnbr:JjdIKNTvtgX0JKFp2cSz3
MD5:	89BA4E29DC7A63CD15959A5BB068BB0E
SHA1:	250DEBBAEE6E7DC0C79F2BF23D8C84512F03BC10
SHA-256:	3ADC584FB0BEF1FBF9B1C0ECDDDE5727643B4334C734DB78B517AB112D92E1D8
SHA-512:	B7297EE98B51B5E8113CF1E50A8081B82B1A9AED9B386322AADB8CD4689D2C3335AF1858211615DB024AAA47FA3DE9E4C568D145D1C23AC45A7E20EA074D249
Malicious:	false
Reputation:	low
IE Cache URL:	http://fonts.gstatic.com/s/opensans/v20/mem8YaGs126MiZpBA-U1UQ.woff
Preview:	wOFF.....l<.....GDEF.....-....4.qGPOS.....GSUB.....>.w.:OS/2...x..._...`.6..cmap.....h.....cvt ...@...Y.....M..fpgm.....~a..gasp...8.....#glyf...H.....'...A.head.....6...6..cphhea...,... ...$...Phmtx...L.....k.2.loca.....tmaxp..... ... . ..name.....&:A.post.....B...@...prep...,.....C...x.c`d``.a..&.V .....$...../s..#s.s..#. .....x.U..n.P.D.....am.QmcK.....L.@g.w.$....MWS.87SM+....@..8"".y.0RI;;>.f..^.1..W.....w\...p.0@...I..v.. ...m"D...1.....L..v7*P!.D..U.....t.)..f..1..|.....Y..B..WF.+[...x.c`f..8.....u..1...<.f.....{...h..... 0t.vf.....&.O.....)B..q>H..u..R``.....1.x.....;....L.j.Ms[.m.m..P.m....v.ijkb..... 8p...;.;..y!?.....a<L.5..v.8...}4,.K..]l.....Q..E.h....4.&...Cs. ...<./.....|.....C...(..>b..+..G.E."2.. .td\.\...ef.[6..d79]..}...."....%.Uu.....Du.....Tw.....{.hc.@ZGA....0..TX.k[.d\d./Y.w...q.:....;.P.H.c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\suspendedpage[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\suspendedpage[1].htm

Size (bytes):	888
Entropy (8bit):	4.965967738451432
Encrypted:	false
SSDEEP:	12:hYEy722CnddmNWprzaSbZUAEdYXg2y/rPMYWjd3wbt7iLV7FzVKiw/LLGL:hYECpC3mNYbZZEWXXyTPMYWx3ut88dnu
MD5:	998BED8BB5FB5A2207B8D94268D1E0B9
SHA1:	58F3F1208B7D8D2FD0298DD804EBAB5D3D91B40C
SHA-256:	4DD3D615813A715CD47725CE1AFC19BA31787B11523081A307288A1AA0AD509C
SHA-512:	2C4626646FC8A48344C6DE7C470A4CB5C956690EBCD34AECB5418AB29FE2866075838352B413CAB34125D00FA55F5C10D40815E839C31192CA2072CFCB61452
Malicious:	false
Reputation:	low
IE Cache URL:	http://covid19.iqwasithealth.com/cgi-sys/suspendedpage.cgi
Preview:	<!DOCTYPE html>.<html lang="en">.. <head>. <meta charset="UTF-8">. <meta name="viewport" content="width=device-width, initial-scale=1.0">. <link rel=" stylesheet" href="//bluehost-cdn.com/media/user/suspended_account/_bh/suspended.css">. <link rel="preconnect" href="//fonts.gstatic.com">. <link href="//fonts.googl eapis.com/css2?family=Open+Sans:wght@300;400&display=swap" rel="stylesheet">. </head>.. <body>. <div>. <img class="suspend-photo" src="//bluehost-cdn. com/media/user/suspended_account/_bh/beback-soon.png" alt="Be back soon photo">. <h2 class="be-back">Be back soon!</h2>. <p class="website-m oved">This website is under maintenance.</br>Check back tomorrow!</p>. </br>. <p class="questions">*If you.re the owner of this website and have questions, reach out to Bluehost. We.re happy to help.</p>. </div>. </body>..</html>.

C:\Users\user\AppData\Local\Temp\~DF0730CF74CFD88E68.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4801790696040825
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loTF9lo59lWYSeW:kBqoIicYSeW
MD5:	40DE297BCDC8C3AB98F8DBA30F15F24B
SHA1:	896318F6F80C29040E69F0A4260A3FBB60E0AB5A
SHA-256:	35B195DA5DC569ABA1293CC861266B70A3D93075BCFB6B3F73215E6308DFDC67
SHA-512:	85EFFC9110BF67A387E564A4392077FC147291A6E275F1B7A0A6B4C2A7E4DFA0CC0CCFDD21B196DBDF6C862BCDCBAAF75E9CEC7B0D3120F58C839FE8B75AE 32A
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF2D0378F71AA387A3.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34421
Entropy (8bit):	0.360954660571928
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwr9lwr9l2d9l2d9l/lg:kBqoxKAuvScS+0SYplIl7njDMA
MD5:	56170A3363A7CADC44EF96562571AA2C
SHA1:	7DFC500196A0C0A6E1BC5E0B1656B353BAF6BD22
SHA-256:	4DDD3710102A5DD532534035E2F6C51C2FF6F31498577C046D7070FE4A406697
SHA-512:	F8840CCB5E3502CC0F95A57CD821324E7A86930C1A763526335AEDB5C6962E361F070D2702716B74DCBD3A881599FC1BC31019A8BDAA08A369171CEE18A8F59
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFF1FEBD55FD9ECCDE.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A

C:\Users\user\AppData\Local\Temp\~DFF1FEBD55FD9ECCDE.TMP	
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 90

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

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 29, 2021 01:26:50.245557070 CEST	49716	80	192.168.2.3	50.87.248.41
May 29, 2021 01:26:50.245640993 CEST	49717	80	192.168.2.3	50.87.248.41
May 29, 2021 01:26:50.434864044 CEST	80	49717	50.87.248.41	192.168.2.3
May 29, 2021 01:26:50.434905052 CEST	80	49716	50.87.248.41	192.168.2.3
May 29, 2021 01:26:50.434972048 CEST	49717	80	192.168.2.3	50.87.248.41
May 29, 2021 01:26:50.435025930 CEST	49716	80	192.168.2.3	50.87.248.41
May 29, 2021 01:26:50.435770988 CEST	49717	80	192.168.2.3	50.87.248.41
May 29, 2021 01:26:50.630662918 CEST	80	49717	50.87.248.41	192.168.2.3
May 29, 2021 01:26:50.636162996 CEST	80	49717	50.87.248.41	192.168.2.3
May 29, 2021 01:26:50.636281013 CEST	49717	80	192.168.2.3	50.87.248.41
May 29, 2021 01:26:50.642522097 CEST	49717	80	192.168.2.3	50.87.248.41
May 29, 2021 01:26:50.873291016 CEST	80	49717	50.87.248.41	192.168.2.3
May 29, 2021 01:26:50.900831938 CEST	80	49717	50.87.248.41	192.168.2.3
May 29, 2021 01:26:50.901034117 CEST	49717	80	192.168.2.3	50.87.248.41
May 29, 2021 01:26:51.044325113 CEST	49718	80	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.045214891 CEST	49719	80	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.089591026 CEST	80	49718	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.089713097 CEST	49718	80	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.090150118 CEST	49718	80	192.168.2.3	52.29.153.112

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 29, 2021 01:26:51.090699911 CEST	80	49719	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.090854883 CEST	49719	80	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.091206074 CEST	49719	80	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.135221958 CEST	80	49718	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.135267019 CEST	80	49718	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.135363102 CEST	49718	80	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.136833906 CEST	80	49719	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.136867046 CEST	80	49719	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.136949062 CEST	49719	80	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.141592979 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.144335985 CEST	49723	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.186923027 CEST	443	49722	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.187051058 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.189831972 CEST	443	49723	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.189950943 CEST	49723	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.192143917 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.192147970 CEST	49723	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.234410048 CEST	443	49723	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.234452009 CEST	443	49722	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.235543013 CEST	443	49723	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.235586882 CEST	443	49723	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.235610962 CEST	49723	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.235625982 CEST	443	49723	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.235635042 CEST	49723	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.235665083 CEST	443	49723	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.235680103 CEST	49723	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.235716105 CEST	443	49722	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.235730886 CEST	49723	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.235759020 CEST	443	49722	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.235789061 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.235797882 CEST	443	49722	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.235826015 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.235836029 CEST	443	49722	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.235841990 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.235887051 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.290298939 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.290477991 CEST	49723	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.295983076 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.296168089 CEST	49723	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.296176910 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.296308041 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.332789898 CEST	443	49723	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.332811117 CEST	443	49723	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.332818985 CEST	443	49722	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.332885027 CEST	443	49722	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.332978010 CEST	49723	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.333023071 CEST	49723	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.333029032 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.333062887 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.333591938 CEST	49723	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.334291935 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.338377953 CEST	443	49723	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.338392019 CEST	443	49722	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.338462114 CEST	49723	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.338499069 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.338537931 CEST	443	49722	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.338665009 CEST	443	49722	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.338731050 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:51.419467926 CEST	443	49723	52.29.153.112	192.168.2.3
May 29, 2021 01:26:51.419502020 CEST	443	49722	52.29.153.112	192.168.2.3
May 29, 2021 01:26:52.134283066 CEST	443	49722	52.29.153.112	192.168.2.3
May 29, 2021 01:26:52.134339094 CEST	443	49722	52.29.153.112	192.168.2.3
May 29, 2021 01:26:52.134380102 CEST	443	49722	52.29.153.112	192.168.2.3
May 29, 2021 01:26:52.134413004 CEST	49722	443	192.168.2.3	52.29.153.112

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 29, 2021 01:26:52.134418011 CEST	443	49722	52.29.153.112	192.168.2.3
May 29, 2021 01:26:52.134449005 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:52.134455919 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:52.134459972 CEST	443	49722	52.29.153.112	192.168.2.3
May 29, 2021 01:26:52.134460926 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:52.134500027 CEST	443	49722	52.29.153.112	192.168.2.3
May 29, 2021 01:26:52.134510040 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:52.134550095 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:52.134552002 CEST	443	49722	52.29.153.112	192.168.2.3
May 29, 2021 01:26:52.134598017 CEST	443	49722	52.29.153.112	192.168.2.3
May 29, 2021 01:26:52.134604931 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:52.134637117 CEST	443	49722	52.29.153.112	192.168.2.3
May 29, 2021 01:26:52.134651899 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:52.134677887 CEST	443	49722	52.29.153.112	192.168.2.3
May 29, 2021 01:26:52.134685993 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:52.134723902 CEST	49722	443	192.168.2.3	52.29.153.112
May 29, 2021 01:26:52.177011967 CEST	443	49722	52.29.153.112	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 29, 2021 01:26:42.610455990 CEST	64185	53	192.168.2.3	8.8.8.8
May 29, 2021 01:26:42.668370008 CEST	53	64185	8.8.8.8	192.168.2.3
May 29, 2021 01:26:43.436427116 CEST	65110	53	192.168.2.3	8.8.8.8
May 29, 2021 01:26:43.491252899 CEST	53	65110	8.8.8.8	192.168.2.3
May 29, 2021 01:26:44.406733990 CEST	58361	53	192.168.2.3	8.8.8.8
May 29, 2021 01:26:44.464737892 CEST	53	58361	8.8.8.8	192.168.2.3
May 29, 2021 01:26:45.320705891 CEST	63492	53	192.168.2.3	8.8.8.8
May 29, 2021 01:26:45.381988049 CEST	53	63492	8.8.8.8	192.168.2.3
May 29, 2021 01:26:46.174309969 CEST	60831	53	192.168.2.3	8.8.8.8
May 29, 2021 01:26:46.235430002 CEST	53	60831	8.8.8.8	192.168.2.3
May 29, 2021 01:26:47.197685957 CEST	60100	53	192.168.2.3	8.8.8.8
May 29, 2021 01:26:47.250341892 CEST	53	60100	8.8.8.8	192.168.2.3
May 29, 2021 01:26:47.981488943 CEST	53195	53	192.168.2.3	8.8.8.8
May 29, 2021 01:26:48.033015966 CEST	53	53195	8.8.8.8	192.168.2.3
May 29, 2021 01:26:48.892121077 CEST	50141	53	192.168.2.3	8.8.8.8
May 29, 2021 01:26:48.942276001 CEST	53	50141	8.8.8.8	192.168.2.3
May 29, 2021 01:26:49.186651945 CEST	53023	53	192.168.2.3	8.8.8.8
May 29, 2021 01:26:49.246287107 CEST	53	53023	8.8.8.8	192.168.2.3
May 29, 2021 01:26:50.174695015 CEST	49563	53	192.168.2.3	8.8.8.8
May 29, 2021 01:26:50.180499077 CEST	51352	53	192.168.2.3	8.8.8.8
May 29, 2021 01:26:50.235613108 CEST	53	49563	8.8.8.8	192.168.2.3
May 29, 2021 01:26:50.240751982 CEST	53	51352	8.8.8.8	192.168.2.3
May 29, 2021 01:26:50.980010033 CEST	59349	53	192.168.2.3	8.8.8.8
May 29, 2021 01:26:50.987152100 CEST	57084	53	192.168.2.3	8.8.8.8
May 29, 2021 01:26:51.042885065 CEST	53	59349	8.8.8.8	192.168.2.3
May 29, 2021 01:26:51.056365013 CEST	53	57084	8.8.8.8	192.168.2.3
May 29, 2021 01:26:51.152918100 CEST	58823	53	192.168.2.3	8.8.8.8
May 29, 2021 01:26:51.202640057 CEST	53	58823	8.8.8.8	192.168.2.3
May 29, 2021 01:26:51.358534098 CEST	57568	53	192.168.2.3	8.8.8.8
May 29, 2021 01:26:51.424640894 CEST	53	57568	8.8.8.8	192.168.2.3
May 29, 2021 01:26:53.454166889 CEST	50540	53	192.168.2.3	8.8.8.8
May 29, 2021 01:26:53.517425060 CEST	53	50540	8.8.8.8	192.168.2.3
May 29, 2021 01:26:54.387747049 CEST	54366	53	192.168.2.3	8.8.8.8
May 29, 2021 01:26:54.437839031 CEST	53	54366	8.8.8.8	192.168.2.3
May 29, 2021 01:26:55.327464104 CEST	53034	53	192.168.2.3	8.8.8.8
May 29, 2021 01:26:55.382652998 CEST	53	53034	8.8.8.8	192.168.2.3
May 29, 2021 01:26:56.262373924 CEST	57762	53	192.168.2.3	8.8.8.8
May 29, 2021 01:26:56.322027922 CEST	53	57762	8.8.8.8	192.168.2.3
May 29, 2021 01:26:57.207361937 CEST	55435	53	192.168.2.3	8.8.8.8
May 29, 2021 01:26:57.259989023 CEST	53	55435	8.8.8.8	192.168.2.3
May 29, 2021 01:26:58.680455923 CEST	50713	53	192.168.2.3	8.8.8.8
May 29, 2021 01:26:58.740778923 CEST	53	50713	8.8.8.8	192.168.2.3
May 29, 2021 01:27:00.193970919 CEST	56132	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 29, 2021 01:27:00.252892971 CEST	53	56132	8.8.8.8	192.168.2.3
May 29, 2021 01:27:07.154336929 CEST	58987	53	192.168.2.3	8.8.8.8
May 29, 2021 01:27:07.310522079 CEST	53	58987	8.8.8.8	192.168.2.3
May 29, 2021 01:27:15.562521935 CEST	56579	53	192.168.2.3	8.8.8.8
May 29, 2021 01:27:15.634840012 CEST	53	56579	8.8.8.8	192.168.2.3
May 29, 2021 01:27:19.186604977 CEST	60633	53	192.168.2.3	8.8.8.8
May 29, 2021 01:27:19.236835003 CEST	53	60633	8.8.8.8	192.168.2.3
May 29, 2021 01:27:19.856971025 CEST	61292	53	192.168.2.3	8.8.8.8
May 29, 2021 01:27:19.907697916 CEST	53	61292	8.8.8.8	192.168.2.3
May 29, 2021 01:27:20.175225973 CEST	60633	53	192.168.2.3	8.8.8.8
May 29, 2021 01:27:20.226283073 CEST	53	60633	8.8.8.8	192.168.2.3
May 29, 2021 01:27:20.847006083 CEST	61292	53	192.168.2.3	8.8.8.8
May 29, 2021 01:27:20.898063898 CEST	53	61292	8.8.8.8	192.168.2.3
May 29, 2021 01:27:21.191365957 CEST	60633	53	192.168.2.3	8.8.8.8
May 29, 2021 01:27:21.241616964 CEST	53	60633	8.8.8.8	192.168.2.3
May 29, 2021 01:27:21.862235069 CEST	61292	53	192.168.2.3	8.8.8.8
May 29, 2021 01:27:21.912525892 CEST	53	61292	8.8.8.8	192.168.2.3
May 29, 2021 01:27:23.206593990 CEST	60633	53	192.168.2.3	8.8.8.8
May 29, 2021 01:27:23.257946968 CEST	53	60633	8.8.8.8	192.168.2.3
May 29, 2021 01:27:23.842329979 CEST	63619	53	192.168.2.3	8.8.8.8
May 29, 2021 01:27:23.878057003 CEST	61292	53	192.168.2.3	8.8.8.8
May 29, 2021 01:27:23.929691076 CEST	53	61292	8.8.8.8	192.168.2.3
May 29, 2021 01:27:23.940299034 CEST	53	63619	8.8.8.8	192.168.2.3
May 29, 2021 01:27:27.222063065 CEST	60633	53	192.168.2.3	8.8.8.8
May 29, 2021 01:27:27.272456884 CEST	53	60633	8.8.8.8	192.168.2.3
May 29, 2021 01:27:27.894042969 CEST	61292	53	192.168.2.3	8.8.8.8
May 29, 2021 01:27:27.944314003 CEST	53	61292	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 29, 2021 01:26:50.174695015 CEST	192.168.2.3	8.8.8.8	0x1eaf	Standard query (0)	covid19.iq wasithealth.com	A (IP address)	IN (0x0001)
May 29, 2021 01:26:50.980010033 CEST	192.168.2.3	8.8.8.8	0xb63e	Standard query (0)	bluehost-cdn.com	A (IP address)	IN (0x0001)
May 29, 2021 01:27:07.154336929 CEST	192.168.2.3	8.8.8.8	0x6fc9	Standard query (0)	covid19.iq wasithealth.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 29, 2021 01:26:50.235613108 CEST	8.8.8.8	192.168.2.3	0x1eaf	No error (0)	covid19.iq wasithealth.com		50.87.248.41	A (IP address)	IN (0x0001)
May 29, 2021 01:26:51.042885065 CEST	8.8.8.8	192.168.2.3	0xb63e	No error (0)	bluehost-cdn.com		52.29.153.112	A (IP address)	IN (0x0001)
May 29, 2021 01:27:07.310522079 CEST	8.8.8.8	192.168.2.3	0x6fc9	No error (0)	covid19.iq wasithealth.com		50.87.248.41	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- covid19.iqwasithealth.com
  - bluehost-cdn.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49717	50.87.248.41	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 29, 2021 01:26:50.435770988 CEST	1177	OUT	GET /jillian-ratke-iii/kathy_edler-43.zip 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: covid19.iqwasithealth.com Connection: Keep-Alive
May 29, 2021 01:26:50.636162996 CEST	1185	IN	HTTP/1.1 302 Found Date: Fri, 28 May 2021 23:26:50 GMT Server: Apache Location: http://covid19.iqwasithealth.com/cgi-sys/suspendedpage.cgi Content-Length: 242 Keep-Alive: timeout=5, max=75 Connection: Keep-Alive 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 3a 2f 2f 63 6f 76 69 64 31 39 2e 69 71 77 61 73 69 74 68 65 61 6c 74 68 2e 63 6f 6d 2f 63 67 69 2d 73 79 73 2f 73 75 73 70 65 6e 64 65 64 70 61 67 65 2e 63 67 69 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>
May 29, 2021 01:26:50.642522097 CEST	1185	OUT	GET /cgi-sys/suspendedpage.cgi 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: covid19.iqwasithealth.com Connection: Keep-Alive
May 29, 2021 01:26:50.900831938 CEST	1190	IN	HTTP/1.1 200 OK Date: Fri, 28 May 2021 23:26:50 GMT Server: Apache Vary: Accept-Encoding Content-Encoding: gzip host-header: c2hhcmVkLmJsdWVob3N0LmNvbQ== Content-Length: 497 Keep-Alive: timeout=5, max=74 Connection: Keep-Alive Content-Type: text/html Data Raw: 1f 8b 08 00 00 00 00 00 03 9d 52 cb 8e d4 30 10 bc cf 57 f4 fa c0 01 36 c9 30 70 40 90 04 b4 0b 48 9c 16 89 41 88 d3 aa 63 f7 c4 d6 fa 85 ed 4c 94 1b bf c1 ef ed 97 e0 cc 8b 81 b9 71 4a b9 5d ae aa ee 4e 7d f5 fe ee 76 fd fd f3 07 90 c9 e8 76 51 cf 1f d0 68 fb 86 91 65 ed 62 01 50 4b 42 d1 66 90 a1 a1 84 c0 25 86 48 a9 61 5f d7 1f 8b 57 ec fc ca a2 a1 86 6d 15 8d de 85 c4 80 3b 9b c8 66 ea a8 44 92 8d a0 ad e2 54 ec 0e d7 a0 ac 4a 0a 75 11 39 6a 6a 9e 97 cb a3 94 56 f6 01 02 e9 86 c5 34 69 8a 92 28 6b c9 40 9b 86 55 55 a7 07 92 2e a6 82 0b 5b 72 67 2a 43 42 61 35 44 0a 55 1c a2 27 2b 48 dc 23 e7 6e b0 a9 ba ef e4 9f 6a c9 63 bc 34 f1 81 72 4e 4b fc cc 64 93 83 c7 b2 8f 09 93 e2 b3 cb 5f cf fe 61 39 d7 6b 42 af e2 2e 4e f6 58 bd dd a0 51 7a 6a ee b2 ef b3 2f 68 e3 eb b1 97 e9 dd 8b e5 f2 cd cb e5 f2 89 50 d1 6b 9c 9a 38 a2 67 17 9d ce 4e 75 b5 9f fa 0c 3b 27 a6 83 bb 50 db 3d ca 58 99 1e b8 c6 18 f3 e3 7d 83 85 97 2e 39 06 31 f0 ff 1b 54 47 1d f2 87 22 3a 67 4b 6f 7b 06 a8 f3 ee 6e 08 e6 32 cc 65 d8 5b 9c 42 c8 d5 31 43 47 c5 cc 62 ed 39 fd 2a f7 b1 3a 91 fd 91 3b 52 17 55 a2 c2 b8 2d 09 d6 ae a5 8a 70 a8 41 86 43 0e 16 c0 a0 9a 7f 1e b4 9c ca ba ea 42 7b 2b 29 cb ee b4 93 33 2e 04 37 66 7d 7f 92 9f 39 17 56 3f 06 8a 49 39 9b f7 fe f4 d3 06 26 37 3c fe fc 15 08 92 24 70 a3 cd 3e 6e 93 0f 67 01 d0 0a 90 b8 25 38 3d bd ce 2b 42 2e c1 0d 29 3b c3 cd 61 ae 25 7c a3 bd 98 44 ef a7 f9 4a 92 f6 e5 29 53 5d 1d f6 95 a3 ed 76 b8 c8 e3 48 46 b7 8b df 9a 24 1b 73 78 03 00 00 Data Ascii: R0W60p@HAcLqJ]N}vvQhebPKBf%Ha_Wm;fDTJu9jjV4i(k@UU.[rg*CBa5DU'+H#njc4rNKd_a9kB.NXQzj/hPk8 gNu;'P=X}.91TG":gKo{n2e[B1CGb9*:;RU-pACB{+)3.7f}9V?I9&7<$p>ng%8=+B.);a%\|DJ)S]vHF$sx
May 29, 2021 01:26:52.662286997 CEST	1385	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: covid19.iqwasithealth.com Connection: Keep-Alive
May 29, 2021 01:26:52.855429888 CEST	1386	IN	HTTP/1.1 302 Found Date: Fri, 28 May 2021 23:26:52 GMT Server: Apache Location: http://covid19.iqwasithealth.com/cgi-sys/suspendedpage.cgi Content-Length: 242 Keep-Alive: timeout=5, max=73 Connection: Keep-Alive 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 3a 2f 2f 63 6f 76 69 64 31 39 2e 69 71 77 61 73 69 74 68 65 61 6c 74 68 2e 63 6f 6d 2f 63 67 69 2d 73 79 73 2f 73 75 73 70 65 6e 64 65 64 70 61 67 65 2e 63 67 69 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	192.168.2.3	49718	52.29.153.112	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 29, 2021 01:26:51.090150118 CEST	1192	OUT	GET /media/user/suspended_account/_bh/beback-soon.png HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: http://covid19.iqwasithealth.com/cgi-sys/suspendedpage.cgi 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: bluehost-cdn.com Connection: Keep-Alive
May 29, 2021 01:26:51.135267019 CEST	1194	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Fri, 28 May 2021 23:26:51 GMT Content-Type: text/html Content-Length: 162 Connection: keep-alive Location: https://bluehost-cdn.com/media/user/suspended_account/_bh/beback-soon.png Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49719	52.29.153.112	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 29, 2021 01:26:51.091206074 CEST	1192	OUT	GET /media/user/suspended_account/_bh/suspended.css HTTP/1.1 Accept: text/css, */* Referer: http://covid19.iqwasithealth.com/cgi-sys/suspendedpage.cgi 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: bluehost-cdn.com Connection: Keep-Alive
May 29, 2021 01:26:51.136867046 CEST	1194	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Fri, 28 May 2021 23:26:51 GMT Content-Type: text/html Content-Length: 162 Connection: keep-alive Location: https://bluehost-cdn.com/media/user/suspended_account/_bh/suspended.css Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49734	50.87.248.41	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 29, 2021 01:27:07.500947952 CEST	1477	OUT	GET /favicon.ico HTTP/1.1 User-Agent: AutoIt Host: covid19.iqwasithealth.com
May 29, 2021 01:27:07.693190098 CEST	1477	IN	HTTP/1.1 302 Found Date: Fri, 28 May 2021 23:27:07 GMT Server: Apache Location: http://covid19.iqwasithealth.com/cgi-sys/suspendedpage.cgi Content-Length: 242 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 3a 2f 2f 63 6f 76 69 64 31 39 2e 69 71 77 61 73 69 74 68 65 61 6c 74 68 2e 63 6f 6d 2f 63 67 69 2d 73 79 73 2f 73 75 73 70 65 6e 64 65 64 70 61 67 65 2e 63 67 69 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>

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
May 29, 2021 01:26:51.235665083 CEST	52.29.153.112	443	192.168.2.3	49723	CN=*.bluehost-cdn.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Aug 13 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Wed Aug 24 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
May 29, 2021 01:26:51.235836029 CEST	52.29.153.112	443	192.168.2.3	49722	CN=*.bluehost-cdn.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Aug 13 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Wed Aug 24 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5464 Parent PID: 792

General

Start time:	01:26:48
Start date:	29/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff62ccb0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 4952 Parent PID: 5464

General

Start time:	01:26:49
Start date:	29/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5464 CREDAT:17410 /prefetch:2
Imagebase:	0x1350000
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