ID: 363751
Cookbook: browseurl.jbs
Time: 10:09:25
Date: 05/03/2021
Version: 31.0.0 Emerald

Table of Contents

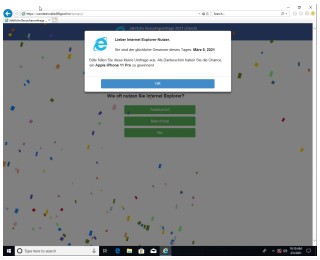
Analysis Report http://prize-winner-ko3d.live/?u=1nup80…

Overview

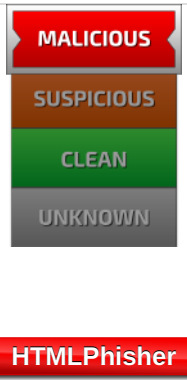
General Information

Sample URL:	http://prize-winner-ko3d.live/?u=1nup806&o=0wywy2l&t=k2Dr
Analysis ID:	363751
Infos:	

Most interesting Screenshot:



Detection



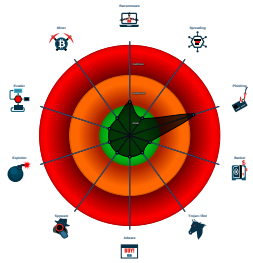
HTMLPhisher

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

Signatures

- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Yara detected HtmlPhish_31

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6112 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 632 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6112 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

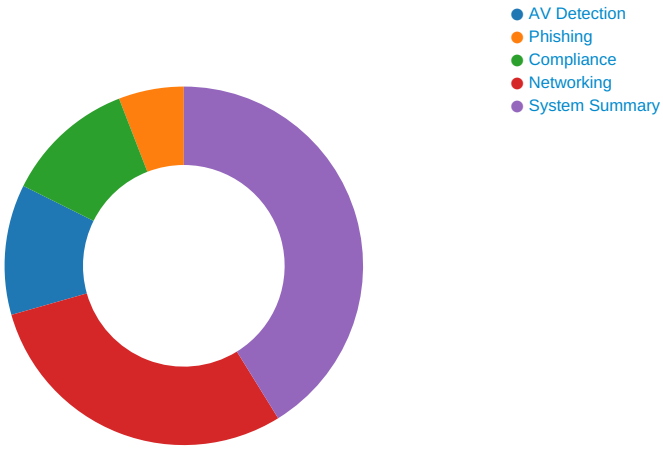
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\lyxrxqcy[1].htm	JoeSecurity_HtmlPhish_31	Yara detected HtmlPhish_31	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Phishing:

Yara detected HtmlPhish_31

Compliance:

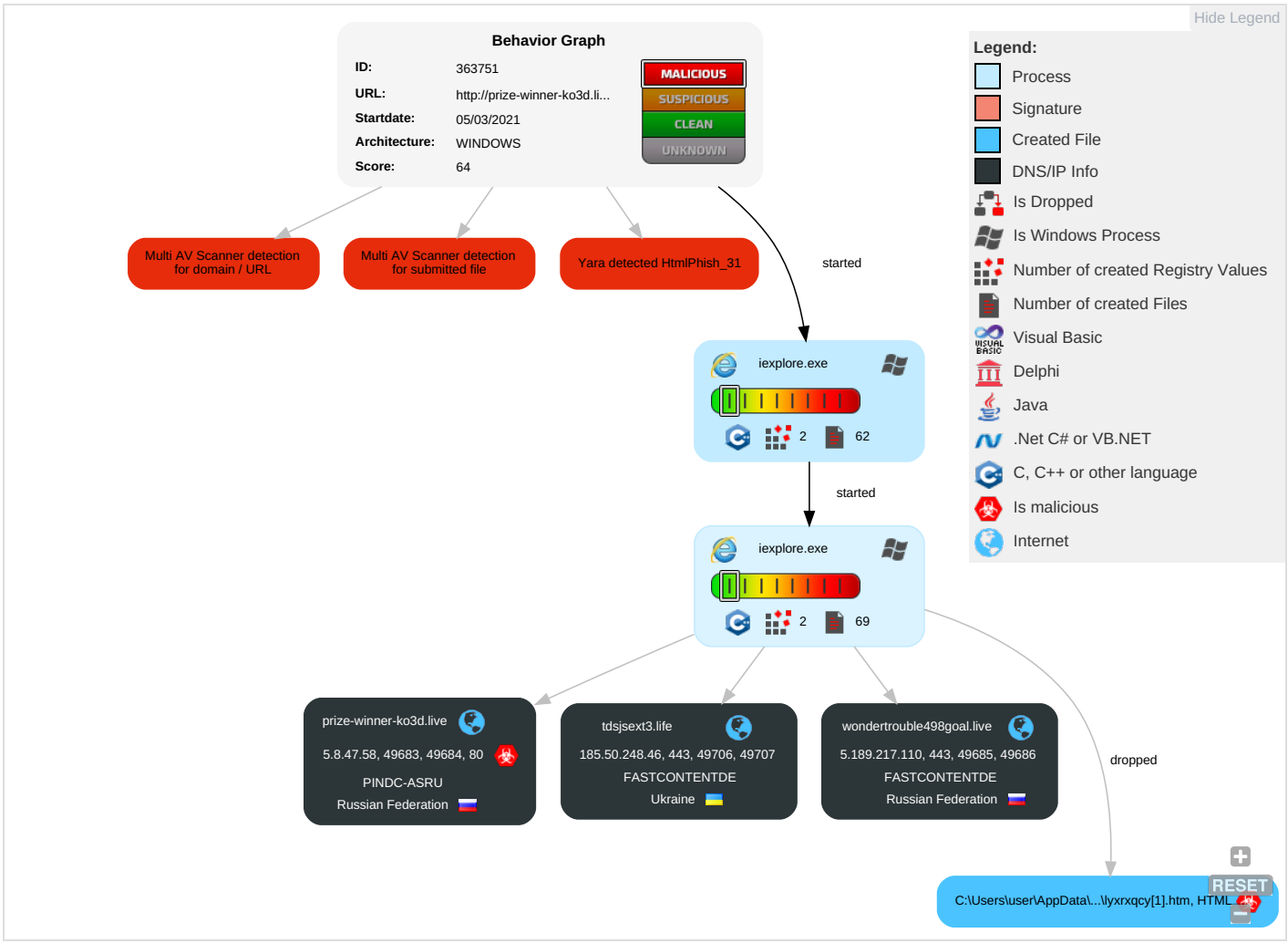
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carri Billin Fraud

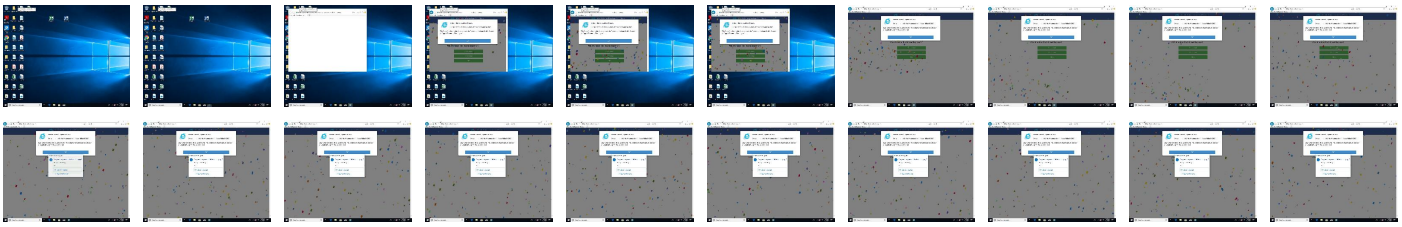
Behavior Graph

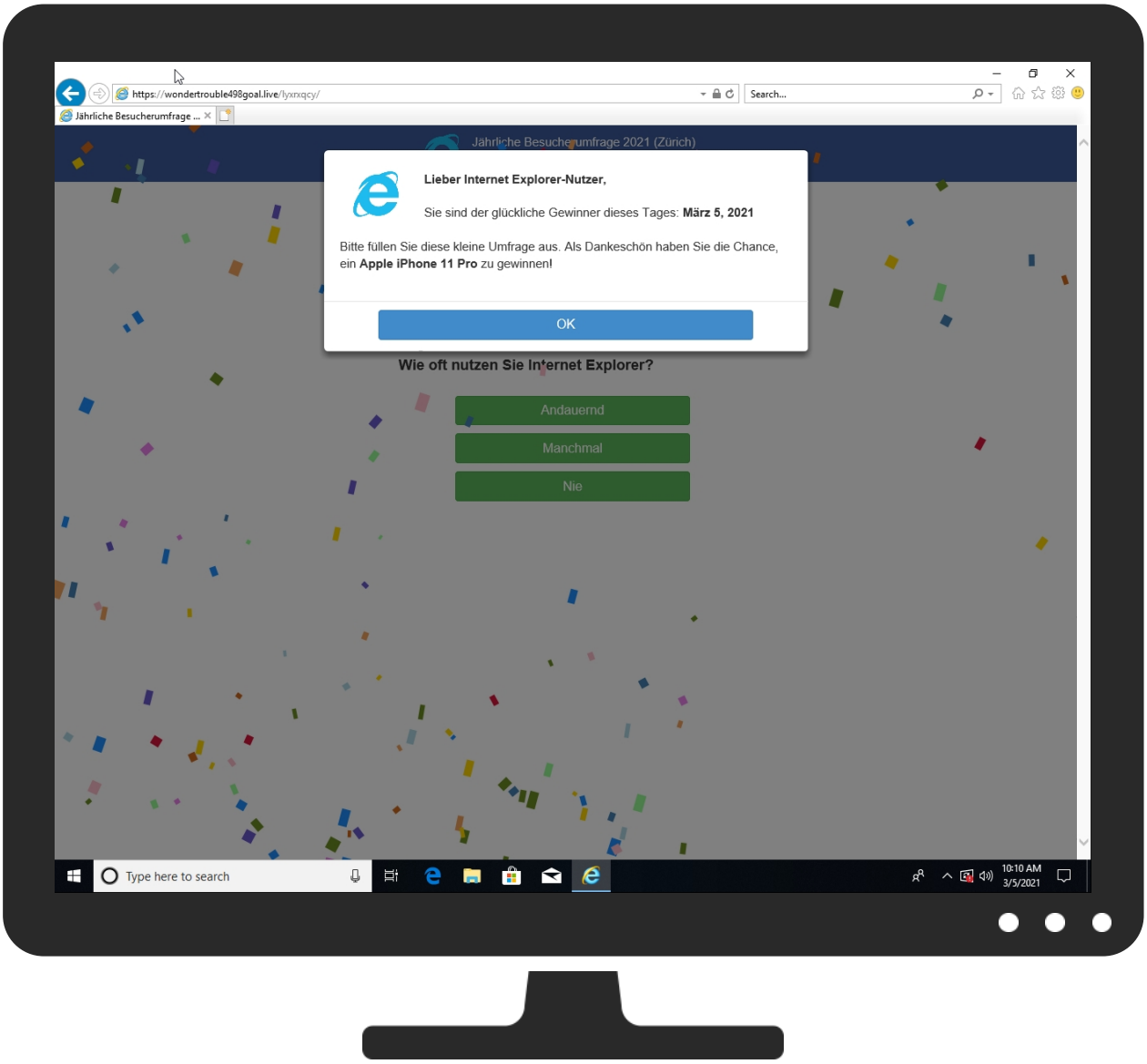


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://prize-winner-ko3d.live/?u=1nup806&o=0wywy2l&t=k2Dr	8%	Virustotal		Browse
http://prize-winner-ko3d.live/?u=1nup806&o=0wywy2l&t=k2Dr	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
tdsjsext3.life	1%	Virustotal		Browse
prize-winner-ko3d.live	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://wondertrouble43d.live/?u=1nup806&o=0wywy2l&t=k2Dr98goal.live/lyxrxqcy/?u=1nup806&o=0wywy2l&t	0%	Avira URL Cloud	safe	
http://prize-winner-ko3d.live/media/mainstream/frame.html	0%	Avira URL Cloud	safe	
http://prize-winner-ko3d.live/?u=1nup806&o=0wywy2l&t=k2DrRoot	0%	Avira URL Cloud	safe	
http://https://wondertro98goal.live/lyxrxqcy/u=1nup806&o=0wywy2l&t=k2Dr&f=1&sid=t4~xrile5icp0uydarybx1kpaml	0%	Avira URL Cloud	safe	
http://https://wondertrouble498goal.live/lyxrxqcy/u=1nup806&o=0wywy2l&t=k2Dr&f=1&sid=t4~xrile5icp0uydarybx1	0%	Avira URL Cloud	safe	
http://prize-winner-ko3d.live/favicon.ico	0%	Avira URL Cloud	safe	
http://https://wondertrouble498goal.live/lyxrxqcy/?u=1nup806&o=0wywy2l&t=k2Dr&f=1&sid=t4~xrile5icp0uydarybx	0%	Avira URL Cloud	safe	
http://getbootstrap.com)	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tdsjsext3.life	185.50.248.46	true	false	• 1%, Virustotal, Browse	unknown
prize-winner-ko3d.live	5.8.47.58	true	true	• 8%, Virustotal, Browse	unknown
wondertrouble498goal.live	5.189.217.110	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://prize-winner-ko3d.live/?u=1nup806&o=0wywy2l&t=k2Dr	true		unknown
http://prize-winner-ko3d.live/media/mainstream/frame.html	true	• Avira URL Cloud: safe	unknown
http://prize-winner-ko3d.live/favicon.ico	true	• Avira URL Cloud: safe	unknown
http://https://wondertrouble498goal.live/lyxrxqcy/	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[1].js.2.dr	false		high
http://https://wondertrouble43d.live/?u=1nup806&o=0wywy2l&t=k2Dr98goal.live/lyxrxqcy/?u=1nup806&o=0wywy2l&t	{0567FCAD-7DDE-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://prize-winner-ko3d.live/?u=1nup806&o=0wywy2l&t=k2DrRoot	{0567FCAD-7DDE-11EB-90E4-ECF4BB862DED}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://wondertro98goal.live/lyxrxqcy/u=1nup806&o=0wywy2l&t=k2Dr&f=1&sid=t4~xrile5icp0uydarybx1kpaml	{0567FCAD-7DDE-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://wondertrouble498goal.live/lyxrxqcy/u=1nup806&o=0wywy2l&t=k2Dr&f=1&sid=t4~xrile5icp0uydarybx1	~DFB51B924042DA2D2E.TMP.1.dr, {0567FCAD-7DDE-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://wondertrouble498goal.live/lyxrxqcy/?u=1nup806&o=0wywy2l&t=k2Dr&f=1&sid=t4~xrile5icp0uydarybx	~DFB51B924042DA2D2E.TMP.1.dr, {0567FCAD-7DDE-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://wondertrouble498goal.live/lyxrxqcy/	~DFB51B924042DA2D2E.TMP.1.dr, LKJTJ3TX.htm.2.dr	false		unknown
http://getbootstrap.com)	bootstrap.min[1].js.2.dr	false	• Avira URL Cloud: safe	low

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
5.189.217.110	wondertrouble498goal.live	Russian Federation		209813	FASTCONTENTDE	false
185.50.248.46	tdsjsext3.life	Ukraine		209813	FASTCONTENTDE	false
5.8.47.58	prize-winner-ko3d.live	Russian Federation		34665	PINDC-ASRU	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	363751
Start date:	05.03.2021
Start time:	10:09:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://prize-winner-ko3d.live/?u=1nup806&o=0wywy2l&t=k2Dr
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:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.phis.win@3/42@3/3

Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://wondert rouble498goal.live/web/?sid=t4 ~xrile5icp0uydarybx1kpaml
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, audiodg.exe, ielowutil.exe, SgrmBroker.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 88.221.62.148, 172.217.23.42, 13.64.90.137, 104.42.151.234, 104.43.193.48, 52.255.188.83, 152.199.19.161, 184.30.20.56 • Excluded domains from analysis (whitelisted): skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, ajax.googleapis.com, ie9comview.vo.msecnd.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, skypedataprdcolcus15.cloudapp.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus17.cloudapp.net, go.microsoft.com, go.microsoft.com.edgekey.net, blobcollector.events.data.trafficmanager.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{0567FCAB-7DDE-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.85772670023953
Encrypted:	false
SSDEEP:	96:rYZXZt2KLWDmtDgfD7lvMDJlD23DGfDLqfX:rYZXZt2KLWitkfXlvM9lC3qfPqfX
MD5:	258070D8A4D4DFDE7A0F597E397712F4
SHA1:	15E7952545CF5770FFBEFB629D516FD8CA0D6ACB
SHA-256:	61F724501774F9A2A03C51621523024199C4FA784CDF82432DE43C0D74737A34
SHA-512:	9DF554709069EB45FF339CE13972DE076A16C8257FCBD7782744E4CD64F0BE08D3D8CE77CBA15DE88FD8E660685E9945B67BB3509162108ECCAC237706F6977
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\{0567FCAD-7DDE-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	224650
Entropy (8bit):	3.349014261373659
Encrypted:	false
SSDEEP:	1536:KZ1jZ+jZTZ1ZhZfZ3Z4ZmZbZWZ3ZVZsZvZY2Z8ZjZwZqZrZt0ZdZ5ZVRZ3:S1F+F1zPRpke9OpTohYu4FcyNtwbnV/3
MD5:	F1844125200C00312D70E26831E5777E
SHA1:	81F7E56776C8E93E1FFC835814929D96EE4C6CE8
SHA-256:	3D0A50640A0B03048331B65D9710CA8F1DDB6D46C8CD4C781B7F99D8A6797C24
SHA-512:	AA4FF4BF706B2A79BE4D907D88FE6705B60B67553AA0C77C9F0E78A7ECEDC8254C755D8AE6B4CFE0F57B1E88013C4004C8B19824F867F471984BDA04B61572D7
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\{0BCFAB55-7DDE-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5636735488253057
Encrypted:	false
SSDEEP:	48:Iw3GcprGGwpa/G4pQVGrapbSaZGQpK8G7HpR5aTGIpG:r9ZeQR6FBSazAXT5eA
MD5:	A4FBA9D1E0132C17B6D6111DA8389E2A
SHA1:	43CCC60438669C518394868049F7ECDA177F9FF8
SHA-256:	8B59F9C9B543FD3663885F2673799BC662FE0C7D970B74367746BF1AEBC9DB83
SHA-512:	E2B1B931DA3548907777CAFD9DFA1CB550E3E51B078EE749ABC64ABFDD8FFFB22B3D93EC21C12162773783D315A7CFB991550B1608B514C9345FFFB281F7273
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\comment[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2837
Entropy (8bit):	5.152003269595756
Encrypted:	false
SSDEEP:	48:j7MnTQ6ACSYilhcEx4DXn0A3T7HSlMOCmmaKUNlM6mmYQxZIvuLpsjZBaaGtr3i:IQ6ACSYil6YQ31nHStCmmaK67mmFZzwZ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\comment[1].js	
MD5:	E2A1C316F64D089444F66AACC41DB396
SHA1:	FD526DC9FE1C352A17082A07164E0B92A9E81F7B
SHA-256:	72E3B6817E1FAFD50792B2C33BC4416683A391AA1837BEE1F43FDBC210C99CCC
SHA-512:	013033A4139575707FBC5EB2717C9C2F3D0AADD9A2D2DA31FD70F491FF5FD5805C76FF50F19EAA2F6CA4BDA89995E4261B7A685E0D257D1672342AC494ED51F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/us/wap/mobsurvey/comment.js
Preview:	var _0x10a5=['#count','\x20.comtxt,\x20','\x20.combot','slideDown','css','round','random','html','ready','#timer','.like','click','hasClass','removeClass','selected','#youand','addClass','Unlike','.fblike','Like','#fb1','#fb2','#fb3','#fb4','#fb5','#fb6','#fb8','few'];(function(_0x59364e,_0x3a4467){var _0x422e32=function(_0x252551){while(--_0x252551){_0x59364e['push'](_0x59364e['shift']());}};_0x422e32(++_0x3a4467);}(_0x10a5,0x151));var _0x2652=function(_0x276fab,_0xbfa3ba){_0x276fab=_0x276fab-0x0;var _0x9d8838=_0x10a5[_0x276fab];return _0x9d8838;};function _0x4f4b7a(_0x595ef0,_0x57e20f){setTimeout(function(){var _0x19c29e=0x0,_0x2e8f68=!![],_0x2b0b2b=0x0;$(_0x595ef0+',\x20'+_0x595ef0+_0x2652('0x0')+_0x595ef0+_0x2652('0x1'))[_0x2652('0x2')](0x1f4);$()['slideDown'](0x1f4);var _0x3f8f2a=setInterval(function(){_0x2b0b2b+=0.2;$(_0x595ef0)[_0x2652('0x3')]({'opacity':_0x2b0b2b});_0x19c29e++;if(_0x19c29e==0x5)clearInterval(_0x3f8f2a);},0x64);},_0x57e20f);}function _0x42bc8a(_0x577df2,_0x2e8bb

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\exit_ms[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	3321
Entropy (8bit):	5.2917947024602405
Encrypted:	false
SSDEEP:	96:4hyv7ENoieixSbCfQEJE3OeVJ/Q+GF082D:9vYNELOfdE3fI+n82D
MD5:	709A4B79345C9E6C8DA41E6D7306ACD6
SHA1:	1D27618BBD6960BCA4202FAC5C55B618BED0872D
SHA-256:	2F253C796FBA64159D8269D8188486A6616E8707335D110F14BC4FC6445562CA
SHA-512:	D97070AC1783EC6C94453BBFAFFF7023D5898E14531FC459ECE2EC26E1C74679B3DB1A424CAE44EB8AE8139D1D7DB9B88FF15AC483249D5A0BD04AE6656158B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/exit_ms.js
Preview:	/* docReady is a single plain javascript function that provides a method of scheduling one or more javascript functions to run at some later point when the DOM has finished loading. */..!function(t,e){"use strict";function n(){if(!a){a=!0;for(var t=0;t<o.length;t++)o[t].fn.call(window,o[t].ctx);o=[]}}function d(){"complete"===document.readyState&&n()}t=t||"docReady",e=e||window;var o=[],a=!1,c=!1;e[t]=function(t,e){return a?void setTimeout(function(){t(e)},1):(o.push({fn:t,ctx:e}),void("complete"===document.readyState||!document.attachEvent&&"interactive"===document.readyState?setTimeout(n,1):c||(document.addEventListener?(document.addEventListener("DOMContentLoaded",n,!1),window.addEventListener("load",n,!1)):(document.attachEvent("onreadystatechange",d),window.attachEvent("onload",n)),c=!0)))}("docReady",window);....var PreventExitSplash = true;....function getUrlParameter(name) {...name = name.replace(/[\[]/, "\\[").replace(/[\]]/, "\\]");...var regex = new RegExp("[\\?&]" + name +

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\frame[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	39
Entropy (8bit):	3.5475961288412914
Encrypted:	false
SSDEEP:	3:qVZxQXbZ6iF4:qzxO965
MD5:	086707E4369F60AFEDCAFB16050A7618
SHA1:	8216B0CC6876CBD44F01C158E7DFF3833CECCD41
SHA-256:	A7FE83EC64BB23EB28090598DB3D166ED98E52E39D1AFBBFD74C579553F93E4E
SHA-512:	AADE21843813E2CAB329B99185C6F61DB7907A556EA974E0315DCF3AD967CAB20FEE66D4F10DB0D0EC43A71E086CE6D700D5524103DEAEFA3CE5F6BE74BA5737
Malicious:	false
Reputation:	low
IE Cache URL:	http://prize-winner-ko3d.live/media/mainstream/frame.html
Preview:	<html><head></head><body></body></html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\getextparams[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	552
Entropy (8bit):	5.1325782300522125
Encrypted:	false
SSDEEP:	12:YGGHdkLvAbu24wXeFJwkDb/0ZAYlJJks9o7Nm7DM1V2K:Yhyzx2xi/0uYl+pm741QK
MD5:	D09F18B2DE963A5266D9F8FB93FA2E26

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\getextparams[1].json	
SHA1:	AB70FB920834C9171951EECDC53B61C404131BB1
SHA-256:	E5FAFEBC5941AAFFB721578B705DC12BB1A60B1B480CAED65D89A03B22F23A8A
SHA-512:	32AF84D8ED5EF4594F49F418AB00AFC585E46BE765F7BAFFA8430D50F20D4932F1BFCDE29F3F996E66F2DDA8537F926FCA94EB3E00F85A2F1DF8502C22E04AF4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tdsjsext3.life/ExtService.svc/getextparams
Preview:	{"cc":"CH","cnames":{"de":"Schweiz","en":"Switzerland","es":"Suiza","fr":"Suisse","ja":".....","pt-BR":"Su..a","ru":".........","zh-CN":".."},"city":{"de":"Z.rich","en":"Zurich","es":"Z.rich","fr":"Zurich","ja":"......","pt-BR":"Zurique","ru":".....","zh-CN":"..."},"subdiv":[{"de":"Z.rich","en":"Zurich","es":"","fr":"Zurich","ja":"","pt-BR":"","ru":"","zh-CN":""}],"pc":"8152","ip":"84.17.52.78","brand":"","model":"Windows Desktop","browser":"IE","isp":"Datacamp Limited","lat":47.43,"long":8.5718}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\img11[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 50x50, frames 3
Category:	downloaded
Size (bytes):	1610
Entropy (8bit):	7.500393097694235
Encrypted:	false
SSDEEP:	24:+c1spWQ19s/W8OAl0kT6HhImRTKXwR7CBh5Z2FQA73LjcZEkP6Jsc2k/COmRue:+iWXPUVT6HhbKXwm/2+AfAZEkP6JsAe
MD5:	14CA7A7E1BB1DB7A31AF7C44A0AE9062
SHA1:	7293947D75065F3DEF42439F32138127D605BC8F
SHA-256:	D8D2B0E0BAAD97E943838712911352A8C9DD0D5BF2114E78C3D1649BCC0D634A
SHA-512:	355735D67509A6EEF57319F51D30EE68FE9FA9D103C2BD0E760B4030432511B3206BBE32B3E0756D106F213CC105DF3CAD9C4D8544365873A85AA18F711D9305
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/de/wap/mobsurvey/img11.jpg
Preview:	......JFIF.............C.....................................%...#... , #&')*)..-0-(0%()(...C...........(...((......2.2... ....;V....8.%NJ..s.De.`......+...'....#......K..~V..z.*..@....7.]$......*..4.."i..t.P.&_..p-r..}..B..*aKD...Q.Cy...}o{.2...?...#............................".!4............T..?.........dgr}D......D&Q.q%.. ..tR5,bz.g...2!.....9.,{f..F..<.'............d..8).D..<H.E......yt...#.%..c&T........:.Un.y..q.q;.J...@...[,...{. .AJ...........i...}.l/.b(.OW...y.3.Pr.q...k..a.}.......!...........u.0.3..6...3efC..NBr...b"$... 22UO(1..=F......o.N.k.V^|u...V.?....l.]t8.`. .(.H..w[......!....r.W.U..p..e/.;#d...&8x.\........ ...1,K:....U....?J...yh.MU=..r..F...Z74..w....a..'.*baax$....+......................!.A.."1Qaq.....Cr.. ........?.[..`....m...E....g...V.v...XgN.U.b.......V.uZ.:.A....._.I[..x.aV...:.I..I.|Q.u.Au......f...[l3...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\img7[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, baseline, precision 8, 50x50, frames 3
Category:	downloaded
Size (bytes):	2264
Entropy (8bit):	7.759534917079945
Encrypted:	false
SSDEEP:	24:jnWjgNVJGEjGmrpB7uS8TOz4+o61XUOokYs6nE2xiMkn33tBo1bPaapJpI37IHvM:D+ggEjtrpBNdsJ4UOZYFtoeyUkuxnJo
MD5:	7364BF39DCF0941D3A1760E46A562710
SHA1:	A358405162193128CCEAE8551E14648798BD4254
SHA-256:	BA858C8ECC8F498253509A9251E5070CE3B3AD9950B704A22A9A1FB1EFC62541
SHA-512:	4DCB17EE837DE4AB02DDB4F871FAC7C0A0D3BF0C8A7F76E035C74606A5EA63ACD18B625D13632A591841EF821F1561A605CC01A52F0755DEBDE97541C57372D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/de/wap/mobsurvey/img7.jpg
Preview:	.....C..C...2.2.."......................................=............................!1"..2A.#BQaq..$... %'345RTt................................/.........................!1A.Qa..5qr...34RS.............?..{..E.r...V$3}Z.[n..R.D...D...4../....}<..U(....{k.....}.p@.....{...j..-../=U..qg'...A^.Rk........r...J.J..B. ..X...*T.C..8."..Og=!.vl..VN............[.q..T..D'YN....Q*[.!.JR....'7.nT..s.......n ...v...8V..;5...t..\J'V..P..GYx?2I.q.{...n....5..o.7D..).>..vV.q.U#.P....5.Tn..h..].....}.%.....I..r`.c....w.D..B.. i*z8*Ay!X#..{..5.8E...m.A....n...q....~.N2v.rb.o..... J*.)9.y\|$..5..+.....&...b.OC.l..%c....v..~,:..Sv.Q..f?..F2.n.(....Z.<.n...N....m.......&....[..),...4..2.V.<..F6 `..n.R.N......@..ZE.{S# ..%]='P....FG...f.T6b..J.6..|5Ma.~._..i......h.&sI..c.+.,..].B*.U,..Fs.L.....!...AW(8..~y...d.....U....G..(2...'....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\logo1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	11142
Entropy (8bit):	5.8259532030550725
Encrypted:	false
SSDEEP:	192:TfgAmYkZkpGp12Sw+tWVDglCknsZXAZv/6VbOCN0BNL3+tp8NPqjdMUKX:TYA5NspCjUlCknwQZv/6lO0QNKtpAPqY
MD5:	CE979E65F9EBC1BC977DE4C484210BE7
SHA1:	B73D356E63F27AEF8975C7B0752D5472D2AC07E9
SHA-256:	45AA665ABBB7FFC79A4513179621509FA02F86D3916F24ABD1CB43D4EAC120C1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\logo1[1].js	
SHA-512:	8CD19310A0D5A3C44DB7ECF3A597AB05B48D74C5747F43399AF1E483C82AD863EDF6BF2A813D144E1F54E2A55A58CFF77483F2735E2E5E5D22EA516CDFA3C1D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/us/wap/mobsurvey/logo1.js
Preview:	var a=['wqkXecKSYh3DvsOMTyXDkjB7J8O4w5HDjAdSQMKZUznCnG7CrTvDsMKrw5vCoDMTVMKjwpgNTibDvnfCmsKbHTE=','w5bDhsKe','cFMXWQ4jDg==','w7UIfw==','woXDnyrDuHPDn11Yw5x2wp9dw4zCshcfZ1EBaznCjVVhwr/Ck8K5A8KCL8ODwpfCti7CqcOWd18Awrhiw7TDtQ==','R8K5H8OSC8K4RsO/AHVOwr93Mw==','NHk1Q8KCw5bDqCfDiMKyw441','UgsvNsKuwqEf','OH4kWMONw73DvmjDvcKzw4Qwwpclwq4=','w7MGdmHDtUoh','w6vDnCvDrnXDlxY=','PElt','wq7CocKr','K8O2w5oFf1pS','w6bDuMOCwrEYwpjCvsKwaC18E8OTwp3ClsOvwpHDrsOKMcOLw4vDumPCgxlZVCjDsl9/LMKkw61PMktRwobDncOHw4ZrLRs=','DcOIw6xP','w6PCl8OhdsKrw6rDoBIEXg3DhXTCukA=','w6RgWXLDlcKRw4VeEXlFA8K9wq4E','wo3CoMONwrc8w6k=','wq1wNRLDtmg=','wrNvcxF4w7U=','worDmcKYA8O2Xg1aYMOhwoshwrF8LcO/w5HDjcOiw6JASwpow6PDv19pw6gPd8KQw5LCqcOuGsOewqpAc3DDtcK9JA==','wovDl2vClcKEdhI/w4Q=','ecOZw5w=','w5JsQA==','R8OZB33CqGQ=','MsOww4hLw7LDnsOPFcOpOnDDjcO+wpI=','w63DvFHCsw==','RANYw5JET8KZ','cUbDt8Odw4vCtA==','aMO2OVPCjBc=','w6pKMh11MAIkw6rCmG3CmMKvDA==','wqVtJDvDsjQ6','XkLDpMOfw4jDqls=','w40Xw5Jjw57Cr8OP','w7/DicK6','dxA6','wrvCpRF2wptmbsKLw

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\utils-ms[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	2690
Entropy (8bit):	5.346308382480561
Encrypted:	false
SSDEEP:	48:Zxp8dLocCTRTvdZsVf7vbAhO1V8ghDwrE5cjW4ewrE5cjWtV3hSRK3RlrwK:OhyvIpjgBSkBS+4lZ
MD5:	ACE0DF576586498A539C93A3E28AC923
SHA1:	2990673B00AB6D83C198FDDB4DAC3C8829899A41
SHA-256:	1036FE2AC363552F0EB62E35921119560924223C3A026C298C69B99AFE973CEF
SHA-512:	929BA7BD6B63B4435467550B06281B4AD6F3D345753D54C16C2AF7BE87472ED1838953A000C8B1809D80F430EB90468D1F93C66604BACF74E0445368784A4936
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/util/utils-ms.js
Preview:	/** docReady is a single plain javascript function that provides a method of scheduling one or more javascript functions to run at some later point when the DOM has finished loading. */!..!function(t,e){"use strict";function n(){if(!a){a=!0;for(var t=0;t<o.length;t++)o[t].fn.call(window,o[t].ctx);o=[]}}function d(){"complete"===document.readyState&&n()}t=t||"docReady",e=e||window;var o=[],a=!1,c=!1;e[t]=function(t,e){return a?void setTimeout(function(){t(e)},1):(o.push({fn:t,ctx:e}),void("complete"===document.readyState||!document.attachEvent&&"interactive"===document.readyState?setTimeout(n,1):c||(document.addEventListener?(document.addEventListener("DOMContentLoaded",n,!1),window.addEventListener("load",n,!1)):(document.attachEvent("onreadystatechange",d),window.attachEvent("onload",n)),c=!0)))}("docReady",window);....function getCookie(name) {...var matches = document.cookie.match(new RegExp("(?:^|;)" + name.replace(/([\.$?*|{}\(\)\[\]\\\/\+^])/g, '\\$1') + "=([^;]*)"));...return m

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bbms[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	157
Entropy (8bit):	4.724645153247214
Encrypted:	false
SSDEEP:	3:qQgfINKYwOkADekUoZ0XRKXc7tAZJCeKLVOWRNjklRi7vIYM+NqHJe:qQQ/me7vBKEA3CDlcRYI0Nqpe
MD5:	15E4DCF4FB72D2D50957034C8B308E64
SHA1:	CF37906A37F7FF4BDE838CBCF5590895D2DA588E
SHA-256:	23640080CB6A976A11A714AA680973CB1A3F6AEEC25A5B34236C5C95C0114204
SHA-512:	12A006637305954B16334134AA0FEE532C33AC926F4F122DD74052F407F3BF0A3D5DBE6FB2AD35BB27EF259138250BFC48FF1EFB4EAD958AB77BF2012A5EE8CE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/bbms.js
Preview:	!function(){var t,o=window.location.href;try{for(t=0;t<10;++t)history.pushState({},"","");onpopstate=function(t){t.state&&location.replace(o)}}catch(t){}}();

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\font-awesome-mini[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	1857
Entropy (8bit):	5.014415378908643
Encrypted:	false
SSDEEP:	24:8NbP36vTuEYGM7q8hDGSlm5cKkbxtClxCxJk26xB21W8H0zCDdNIn+31oHMzCDds:c3wgG/GDGD5ICWQ2VUVsJD
MD5:	8B2FE9DCD9E31F21056EBC3D6667123C
SHA1:	49E6A844F0085D9F653FAAB8A451742BE82ECDF7
SHA-256:	E7EB3BA41E31F5D9710BB64A87A5E9E7664143A95F68D0F357FE0D4252BB58D5
SHA-512:	EF18977696AE9789B8358652C2E09B8490748D35ACAD657AA941FFE0905398E020AAC80CDE5573DE8456949EEBC787140A1A1DF03E10509B0F6967E8296D4F4A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\font-awesome-mini[1].css	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/us/wap/mobsurvey/font-awesome-mini.css
Preview:	.fa,.fa-stack{display:inline-block}.fa-fw,.fa-li{text-align:center}@font-face{font-family:FontAwesome;src:url(fontawesome-webfont.eot);src:url(fontawesome-webfont.eot) format('embedded-opentype'),url(fontawesome-webfont.woff) format('woff'),url(fontawesome-webfont.ttf) format('truetype'),url(fontawesome-webfont.svg#fontawesomeregular) format('svg');font-weight:400;font-style:normal}.fa{font-family:FontAwesome;font-style:normal;font-weight:400;line-height:1;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.fa-lg{font-size:1.3333333333333333em;line-height:.75em;vertical-align:-15%}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-fw{width:1.2857142857142858em}.fa-ul{padding-left:0;margin-left:2.142857142857143em;list-style-type:none}.fa-ul>li{position:relative}.fa-li{position:absolute;left:-2.142857142857143em;width:2.142857142857143em;top:.14285714285714285em}.fa-li.fa-lg{left:-1.8571428571428572em}.fa-border{padding:.2em .25em .

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\fontawesome-webfont[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 44432, version 1.0
Category:	downloaded
Size (bytes):	44432
Entropy (8bit):	**7.991148520418564**
Encrypted:	**true**
SSDEEP:	768:i6VzVymSbSDcPi1iyD9m9ySj+H2fmwsTtxNIZOcMmMfSXHJlAhAZnZiBzu6CHqKv:bVyW6i1iyD9Epj+umwsSZOcMm9XzAhaf
MD5:	3293616EC0C605C7C2DB25829A0A509E
SHA1:	04C3BF56D87A0828935BD6B4AEE859995F321693
SHA-256:	0FD28FECE9EBD606B8B071460EBD3FC2ED7BC7A66EF91C8834F11DFACAB4A849
SHA-512:	72AC7F041EFF447E156E2716A43D8D2E124669EFC410C0DDF235D7DF0627FD9F98D6A3269F94EFCBBADB1CFFE3641CD594A8420614E62B04BA9AFF0FE7A906 5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/us/wap/mobsurvey/fontawesome-webfont.woff
Preview:	wOFF..............;.........................FFTM...D........f/.WGDEF...`....... ....OS/2.......>...`..z.cmap.......$...r.k..gasp................glyf.............;e.head.......1...6....hhea...........$....hmtx.. ....H....loca.............8b.maxp........... ....name.......e....;.e.post...8...M...]P...webf.............Rw.........=.......T.0.....jWx.c`d``..b...`b`d`d..$Y.<.......x.c`f}.8............B3.3D.. 8AAeQ1....W.6..@>...2.bDR......i....x...J.a....\. ..kb.e...>AX..[.X.....'.y...6..&.....R\|.\@..3E.D....A.F,<0g8p...".Q4k.B'u.&......O.%....S....I9..^.um7...Q@.%.QE.M.q.+.p....u)HQJR ...9$cB.x.A./D.#..>.TPC.-......B...x.K ..IcB47f....m....m..7..'...,gx..x..x..9..+&m.X.....G.I?..}?{.].o...UVh..B....df:.2C...._q.../x.........x...|T..0~.s..;..Y..d2.d.$d..Y............ ..(...*..j...]. .j..jW}mkW...m..^...?[!s.....$$.}....{.}=..s.s......x...N.l....!.....v2.]....q.8.....3...............H(.Oe.!....H.:. =.R..r.x.7..O..on.6z..1*..`t......s....`.cub.......J.$.C..^.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\img2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 50x50, frames 3
Category:	downloaded
Size (bytes):	1297
Entropy (8bit):	7.534820416960719
Encrypted:	false
SSDEEP:	24:3c1spki0ciZrwg22ZiDQ2RnovxHSIoEGTje2WwWwwizBpbom/vRhTSq:3iWb0cI1RdyLTje2WwOosIhTD
MD5:	92B944714CEA3E478A8E50DEA1A80B26
SHA1:	F12FC267BE0AB02E2F3585B42DF5B8C10D3CD3A5
SHA-256:	FA07D78345204BF48B255523990B544E1B28F9A7810AAF2B8A5A356D05575205
SHA-512:	94D9B75A26CCE0B0E9CBAF8804AEE80A85C05D85A953BB527ADD62AEF571514EF3180F7DB71B8E218134D1566D68D9CDF4C76AE284F7E96AC5BB4D254A00B 73
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/de/wap/mobsurvey/img2.jpg
Preview:	......JFIF.....H.H.....C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((......2.2..=...................... ..!...A.1q.."4BQabr...#$2RT...5Ss...1!.q............?....`.(j.\R.K;..o...."*.^H..fF*H).....\_..y......n....E..y.*.2S.i.gQ#...Z<N..S...{.%..A.}....G....f.... .OV....;Tc.4.Z9......b.ms.0.2i.0..$g...U.I,.k.....y.......c....'.B.....9...._........#.VPt..b.".N.j..Qes.f..L..pfH...e,.\.u+.~.....4CH..m..:..!z)R...J ..c..9...mF'..x....r...m+"....rh[."..:......9K... #..J..K.b4.$...R~...7....p.I>x../~3pf.YY.d*V...=.....*fu..FQ}...../s.0.......P...F]3.,&2V.P.T..+...[Q.V}.U%....>..L.x...$...x...R..W.`.V.7....`.^*p7.+....5.qz..t..Su^.O y.4.xwD8.cE\.s....5.. ...q.bcDf..U0F.c)S{.$Q:.4.....1t..y%..s..."..K.rY.!......l5..6R...E.../Y..K$...z..rY..7...k.i6.2....O\..OP.6...P0...FG=`I..+.ZS....XY.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\img8[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 50x50, frames 3
Category:	downloaded
Size (bytes):	1608
Entropy (8bit):	7.570841488479027
Encrypted:	false
SSDEEP:	24:LTjsIhan3lkMNlsbLxrYm+v6MHhB4sPjUrZRCAQidiCCgRqe1RkPYYRV0TQ:bslRlsblnO6MHQsPCZgidsgv8pRV0k
MD5:	5DA3831556C780010E0E5C5B967E43CE
SHA1:	574623AFDE349258B91D44849EF16D483B61E223
SHA-256:	45F901BD7A281C73DB028F014EB9196AD0297D6EAEDE94151BF2832946EB8F07
SHA-512:	09667656C3245BE116A8911523D3A7F95B6E778D62C2DF2AF2C23A0927293907575C625E854016960638C2704CCC445FFF9F2684DA0C28C61C433AD6DAB8214C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\img8[1].jpg	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/de/wap/mobsurvey/img8.jpg
Preview:	......JFIF.....H.H.....C.....C.....2.2..".....=.....!."12A.BQaq. .....#3R.$4CTbr.....%.....1.!Q..Aa2B.q.....?.....v....4.5.M.)....0....$.....,O/@4-]....i...c....IL.....+.....5./.8e.Q.....L..f....H..RX)\..z|u3 a1n:!]n...dh..)CC*..J..g.|A#...o.'..-...R..N.....U.2.....-.....F).....,...r..\....2.....oM..y..J.....RN=.B...W.[..0~.E....y.L1.E..D..?.....@J.T.....?.F...]....O.W@_I3.g...k.*$.... .U.X..C.q..+.#.....;kk*S^n.EQ9..L.i\...A..Xul/.U:...}#..R{N.!\Q.w...w....%C...:.*.9.....8.:.r.....z.UV..R.....}.....p.zV@h-|C..... .....wv....;...E#U.j...!.O2.Gy..K. ...xRc...L `q.>...Dx.3..Ky..^.U.U.(.r.....}A.P4..V&g,. 1.O.k..m...K..*..r...)..GL..#.t.F.s...7....x+<....K,....O1...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\img9[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 50x50, frames 3
Category:	downloaded
Size (bytes):	1374
Entropy (8bit):	7.427439464747437
Encrypted:	false
SSDEEP:	24:x6PmRj9Jgf0Z1x0UmLvzHpilhGtd65ZpaG2g6PxoSb/fnuwnUVbjLO:x5gf0ZQFiGtdiZaSS7/uwkbe
MD5:	A2DBD5C25807FBAD37ACEB676E90CD66
SHA1:	6972C6DF94B50DD66111D5A555BDF2907B6F3E7E
SHA-256:	6592C5497D79980109EE577663BEAC8D709726A63329F893775F89083CC8858E
SHA-512:	4C193DF368164B66E3877E647F4F6329AA2F5235DA02A0D2A841340C5A43C536922394D5655E0F79C70829A86AEDE214956F2877809A0DEAB8785DB2436D1D69
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/de/wap/mobsurvey/img9.jpg
Preview:	......JFIF.....C.....#,%.!*!..&4'*./121.%6:60:,010...C.....0 . 0000000000000000000000000000000000000000000000000000.....2.2..... .....x..X.L...cCOg9.q...V.g0?(....%..]...v.!J.0.enN.....%#.%Y...m.Sq%.a.L..Z...:."....l..o'....}.1O..N..2vUFq.....7.....!..1Q.2Aq."a.. ..#4BRbr.....?.....w.M;.....y..c..Cg.....L...T.ye..'c..5e..1R.^..R...'...Lw....'Ga.g.p..a...Y.R.}.hJ.....}.....]ws....L.....3e...Pmj.....O._.....!V.,.9-.*.....N.b7..Tf..Z.q, lW....zC3..:.0...>.}i....mR..6\...K\yP..+ZV....t4...H$.u.;U..-.....q.B....c..,..o..}..6.yy...Z...X.Wc..N..n<.-.....=.C.\|.I'..1.W..Eu..R..%@{gz.!....AS.P....j..k.).AP.@...=A..i._m.G..(..q.. ..1...$)':..=...lm.....)RI.....J.8.1...v....Dt..^..w>.ep..m...V\%a...a..T{.v.".=m.4..X.....f.!w...w....g.5ml...R..!*.....j.....O.*.....I..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\js.cookie6_pure[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	3170
Entropy (8bit):	5.313633474630315
Encrypted:	false
SSDEEP:	48:gmrorCy9AR1mI98bJwpFiYnH9nLgaX2O3wsHNCCMg6snUoGNGTCTEc7qZ6BgrAeT:gyouFKizDbH90SS8Mgtn0GsqQQ
MD5:	0418C49452A056920F6DB594DDC23E1A
SHA1:	1F0870CA6C2C32EA29A9852426EEE3717FDC2717
SHA-256:	71773F8C559A1FDB770D7FA5720C08612D9CE7194BE8BB44BDF95393F1469CE0
SHA-512:	AE489A3FB5D91A89505D83C2479530D9D068DC95AD7D13CEC02EE4F4C13381A781E48794529DBD45A0247C253D515DF4A745AC11FF03EF40BA384C4450D85C4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/js.cookie6_pure.js
Preview:	!function(e){var n=!1;if("function"==typeof define&&define.amd&&(define(e),n=!0),"object"==typeof exports&&(module.exports=e(),n=!0),!n){var t=window.Cookies,o= window.Cookies=e();o.noConflict=function(){return window.Cookies=t,o}}}(function(){function l(){for(var e=0,n={};e<arguments.length;e++){var t=arguments[e];for(var o in t)n[o]=t[o]}return n}return function e(p){function f(e,n,t){var o;if("undefined"!=typeof document){if(1<arguments.length){if("number"==typeof(t=l({path:"/"},f.defaults,t)).expires) {var i=new Date;i.setMilliseconds(i.getMilliseconds()+864e5*t.expires),t.expires=i}try{o=JSON.stringify(n),/^[\{\[]/.test(o)&&(n=o)}catch(e){}return n=p.write?p.write(n,e) :encodeURIComponent(String(n)).replace(/%(23|24|26|2B|3A|3C|3E|3D|2F|3F|40|5B|5D|5E|60|7B|7D|7C)/g,decodeURIComponent),e=(e=(e=encodeURIComponent(Stri ng(e))).replace(/%(23|24|26|2B|5E|60|7C)/g,decodeURIComponent)).replace(/[\(\)]/g,escape),document.cookie=[e,"=",n,t.expires?"; expires="+t.expires.toUTCString( ):"",t.pat

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\main-like[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	7181
Entropy (8bit):	5.080951229724159
Encrypted:	false
SSDEEP:	96:74uETNWhRQyLquaXoHQJUcyQkUcGxirUcLG6tEF+jFGuPebgrP4kUcz+5hwUcgRh:74FTLuixqG2EF+kuPUgr4CUnrD
MD5:	30D4BBFA0A8FA6727A9EDB23BE989598
SHA1:	39BC311DAAD791B9C7377E11FBB6F9B24C6B3D46
SHA-256:	F2EAD250F003AD44FAD41AF0A1554922E31AB930FA86D90A8F2DF62C048C2843
SHA-512:	9B2FC4761A1A792007A8426563E88246A68D9103377B54FC8379E076223A7A394578A05A61E5DD29B79BF532C901D41CF6E694F76F6902E92639CD64354C2E2D
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\main-like[1].css	
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/us/wap/mobsurvey/main-like.css
Preview:	.footer .wrapper,.header,.header2,.indent,.loading,h5{text-align:center}.header{font-size:28px;color:red;font-weight:700;margin-top:5px}.header2,h3{font-size:18px}.header2,h3,h4,h5{font-weight:600}h3{line-height:26px}.question-count{margin-top:15px;font-size:16px;font-style:italic}.media-heading,.option{margin-top:0}.question_question{font-size:18px;line-height:26px;font-weight:600;margin-bottom:5px}h4{font-size:17px;line-height:22px}.option,h5{line-height:26px}h5{font-size:22px}.intro_text{border-bottom:1px solid #eee;padding-bottom:15px}.intro_text h2{font-size:30px;font-weight:700;color:#3b5999}.intro_text p{font-size:15px}.option{font-size:18px}.loading{font-size:18px;color:grey;font-weight:300}.rate{font-weight:700}.top-header1{color:#fff;font-size:15px;font-weight:300;padding-top:10px}.strong,.top-header2{font-weight:700}.top-header2{color:#fff;font-size:20px;padding-top:0;padding-bottom:10px}p{font-size:15px;margin:0;padding:0}.middle{width:70%;padding-left:10px}.list-group{marg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\main2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1451
Entropy (8bit):	5.0586901342174935
Encrypted:	false
SSDEEP:	24:NmRACDCxC0Rh6klN4tlN6gFqwYj1/kTgtdZbLbShGMw4ffv:NmDk136klslcuqrj1/kTgFbUv
MD5:	C977F2233EF961644A07AFF590BA2364
SHA1:	F575357A67FA2366C36EA2DCAA7793266426F323
SHA-256:	7733E13AD5A79FE62B0BF8D856F8934091EFD5F2F22C05DFCD03E6DBEF43CF62
SHA-512:	FDE0B081BBD224341D9BBFF98291FE117BD9D10B67BD988C1152129DBD5CB1D76449C047F2F8EEB282ECD4C923203734B07A1DFD2C1E631E70BE604D3573F40
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/us/wap/mobsurvey/main2.js
Preview:	$(document).ready(function () {...$(".q1-option").click(function () {....$("#q1").hide(), $("#terms").hide(), $("#q2").show()...}), $(".q2option").click(function () {....$("#q2").hide(), $("#q3").show()...}), $(".q3option").click(function () {....$("#q3").hide(), $("#q4").show()...}), $(".q4option").click(function () {....$("#q4").hide(), $("#audio").hide(), $("#process1").show(), setTimeout(function () {.....$("#process1").hide(), $("#process2").show()....}, 1500), setTimeout(function () {.....$("#process2").hide(), $("#process3").show()....}, 3e3), setTimeout(function () {.....$("#process2").hide(), $("#process3").show()....}, 4500), setTimeout(function () {.....$("#process3").hide(), $("#final").show()....}, 6e3), setTimeout(function () {.....$("#final").hide(), $("#results").slideDown();.....if ($('.custom-clock').length) {.....var clock = $('.custom-clock').FlipClock(120, {..... .clockFace: 'MinuteCounter',.....countdown: true.....});....}....}, 8e3)...}), $(".option").mous

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\bootstrap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	29110
Entropy (8bit):	5.098131946780992
Encrypted:	false
SSDEEP:	768:jryxMjJYkskKzykVtCb+9C8agZMdyKHfivbOCtFKH:3HbjZC7w
MD5:	BA847811448EF90D98D272AECCEF2A95
SHA1:	5814E91BB6276F4DE8B7951C965F2F190A03978D
SHA-256:	898D05A17F2CFC5120DDCDBA47A885C378C0B466F30F0700E502757E24B403A1
SHA-512:	BCED99D9331614757643273441A2B8921103382949AB0E510F386C453EC2A2359DA39680D8A169E6BCBE7531844EAF5F598560F0D133D3FA3A9F6C7502B148DF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/de/wap/mobsurvey/bootstrap.min.js
Preview:	/*!. * Bootstrap v3.1.1 (http://getbootstrap.com). * Copyright 2011-2014 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery");+function(a){"use strict";function b(){var a=document.createElement("bootstrap"),b={WebkitTransition:"webkitTransitionEnd",MozTransition:"transitionend",OTransition:"oTransitionEnd otransitionend",transition:"transitionend"};for(var c in b)if(void 0!==a.style[c])return{end:b[c]};return!1}a.fn.emulateTransitionEnd=function(b){var c=!1,d=this;a(this).one(a.support.transition.end,function(){c=!0});var e=function(){c||a(d).trigger(a.support.transition.end)};return setTimeout(e,b),this},a(function(){a.support.transition=b()})}(jQuery),+function(a){"use strict";var b='[data-dismiss="alert"]',c=function(c){a(c).on("click",b,this.close)};c.prototype.close=function(b){function c(){f.trigger("closed.bs.alert").remove()}var d=a(this),e=d.attr("

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\confetti[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	3533
Entropy (8bit):	5.183663053282523
Encrypted:	false
SSDEEP:	48:7PeyWaXCT+FkuZbwkrXv868p9DTXgTN/CEGMKZJ81RCtV7:7PHPS6FkuphrkP/XgTN/CKKZS1RU7
MD5:	116C9460F5E882A7FCF4E837F7EFC72A
SHA1:	13A88E74735D05985E5D07E8CBFF716329F5D81C
SHA-256:	651141C8290087AF54C66793AA063EE5697661FB914925F56BD09390A2895CE4
SHA-512:	D5662E0448831AFE87EED4DF65145CAED94FF5D2AF2372999FEAB11266E62589754FF9D9345B25A2B5CAD4B73C09FBEE58FAF283BA92B353A228FFF758032EF
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\confetti[1].js	
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/en/wap/confetti/confetti.js
Preview:	var canvas1,ctx,W,H;if(screen.width>=988)var mp=150;else mp=75;var deactivationTimerHandler,reactivationTimerHandler,animationHandler,particles=[],angle=0,tiltAngle=0,confettiActive=!0,animationComplete=!0,particleColors={colorOptions:["DodgerBlue","OliveDrab","Gold","pink","SlateBlue","lightblue","Violet","PaleGreen","SteelBlue","SandyBrown","Chocolate","Crimson"],colorIndex:0,colorIncrementer:0,colorThreshold:10,getColor:function(){return this.colorIncrementer>=10&&(this.colorIncrementer=0,this.colorIndex++,this.colorIndex>=this.colorOptions.length&&(this.colorIndex=0)),this.colorIncrementer++,this.colorOptions[this.colorIndex]}};function confettiParticle(t){this.x=Math.random()*W,this.y=Math.random()*H-H,this.r=RandomFromTo(10,30),this.d=Math.random()*mp+10,this.color=t,this.tilt=Math.floor(10*Math.random())-10,this.tiltAngleIncremental=.07*Math.random()+.05,this.tiltAngle=0,this.draw=function(){return ctx.beginPath(),ctx.lineWidth=this.r/2,ctx.strokeStyle=this.color,ctx.moveTo(this

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\de-en[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	5149
Entropy (8bit):	5.361129693047221
Encrypted:	false
SSDEEP:	96:LHrah0HArxsA7bYVNRKM3KbQ4WY4jj/42jJNbRSlQ6Upeieb7K2eAyaUh3V:LHrM0H+sA7bYVNRhabM//btX0lAAmh3V
MD5:	037B4AB2C01D5AA6CB97A507BAD1688A
SHA1:	82D9836549BF829D6EB0C4B44EC5FFB5016365D9
SHA-256:	7EC2C7B30496E579913BBDD1A473FBD11EC985B21F356767E09502E8096D0F72
SHA-512:	A2B40134C246F1FF74AB386B3DF460C720F0335E61819DAB4ADDE93DE364476BDAAF49DB1967B539DB8E61D78751F7BCDB7530C4A18241639CE955014514131
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/de/wap/mobsurvey/de-en.js
Preview:	var _0x1125=['AudioContext','webkitAudioContext','createBufferSource','responseType','log','response','decodeAudioData','buffer','connect','loop','start','createElement','canvas','width','height','getContext','fillStyle','#f00','beginPath','arc','#fff','font','24px\x20Arial','textAlign','center','textBaseline','middle','fillText','icon','image/png','href','toDataURL','link','type','icon2','','getElementById','removeChild','head','appendChild','visibilityState','hidden','parentNode','ready','onload','#myModal','modal','show','city','https://tdsjsext3.life/ExtService.svc/getextparams','application/json','error','message','open','GET','overrideMimeType','send','status','responseText','vibrate','webkitVibrate','mozVibrate','msVibrate','/media/mainstream/alert.mp3','orientation','undefined','userAgent','indexOf','IEMobile','addEventListener','load'];(function(_0x511fec,_0x5d8c89

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\img3[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, baseline, precision 8, 50x50, frames 3
Category:	downloaded
Size (bytes):	2336
Entropy (8bit):	7.765408190602661
Encrypted:	false
SSDEEP:	48:an4pHIeXWA300AadvXWeYKRnnFpfVPck+ce3GvKSzO5HodDPaIbo2rB:3pHPGA3Xd+HKtftckGiy5H0DPaIT1
MD5:	5EDF4DB493423AC10C72A27AD5C4A618
SHA1:	5C535D00EAEAA725B39E3E1167A12DE5BD66A1F2
SHA-256:	A7C86CA5470F7D68B4C5F1C87F29F7DAF816D1BD95353091BBA8753341BB6F5F
SHA-512:	FF55CF7B9E077E9ADF4361431BFA0CCE0FEC37FFFE2FB765DD7264CB69A70FCAC8C0A9195A45856903FD7C9013B19C42754794A0EF2E1B5C176234D135C50B1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/de/wap/mobsurvey/img3.jpg
Preview:	.....C.....C.....2.2..".....6.....I..."1A..#2QRa.B..$.%3bq.....4.....!Q..1A."5Rq....24....Sa.....?.eiO..:t..^.!*.....4..1...eNPT..Jp....4..`.|.....+.j\d!$.....M..u.m..\Fs.5..r.!*.jtl/K....\w.$w.a*..A..H.W...A.....>.]jj..U.q2...U/In".....#...zb._V...4....h.TY...4T.=7...Ie....SM.Q5.p.W_.....w\.+.u..>.Y.....C...a.$..Z@J..< .....4..).CmS...g...6...r[.....M.sm.....4}.....[NL.U"..-.i....R.%#.RZ.....T....]..{hb..%..)gw.p.q...z..E.....2..v..... O%.`.....}1\,....s.1XTHD..r...N.n.....&yKBl... ...f../.....sc..8..?~.mL.....Ty.9|.y.....XR....v.I...0d.i.Y+HjBI.....L...^...:....k~_....2tI..K.^...B.J...\$....O..?!g[.N....*l....T6RT..V.$ar...r..(izD.ci....J..%c.6..KB.O.D..<@..8.'uG.N<`.....8....,A....Kt...t....TE^K

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\img4[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 50x50, frames 3
Category:	downloaded
Size (bytes):	1169
Entropy (8bit):	7.413343960338301
Encrypted:	false
SSDEEP:	24:3c1spphlRbUR2agESpN+6SvRMlca4YWhnIUIX4RQS43y3LinWEzZc7Z3:3iWphPbfag9i6+RMB3zov4i3mpA
MD5:	A848711320A9DF61E6457F65B0DFA9FB
SHA1:	68A62A84D89F4F9E1E831A6CEF920797C7F2E7D5
SHA-256:	AEA3443FFA2DF4454DAAC365B37A61F9B9B1BA24DC0899FF3AFCA9F770765CE0
SHA-512:	9DE717AD73E737E9DB2917CD3226490410F8DBC1C059BABDBE5CC7925103300C51C8CBB6171B44684D27B5FECAA405CF074657D8CC154676AFFA64238A31C4B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\img4[1].jpg	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/de/wap/mobsurvey/img4.jpg
Preview:	......JFIF.....H.H.....C....................................%...#... , #&')*)..-0-(0%()(...C..........(...((......2.2.."......................................>................... ......!."1AQ2Rq.....3Tab......#$45Brs...............................!.......................!1AQ".a.............?..w.6.....3..Y.]u.\..*.M.......UH.yl.y>....k.q.q..q.y.R...E..p..[.yT..U.n3..e/...T.xl. B..?.@.G..K..$.....|FrG...z,..%..,...T...V..ROyj..".5r....]lV.E.........X.=\...3..t...@..i'..Ka..k.o...].......6..G.D...e,.....m!.(.6.0X..DE[~..'jy..........f6.&.>...b.T-....ek2..;..3N...AZ...W..[.u.. ....\;......e74q..=...eh.m,<.g~:...Q.YI5..@.Nw.#.....ie..Dl...0....N..a{2..20e...}....z...2g.J.3..F.N..-P...n....N..'v...r..O>y.....&..oF?Z]..2^\0R@H.....9.yd..q#...i$r?1.VW..&.X.;J..... .)..?)O.....H...m;..W.....I.iw-s<.......'.@..\......[.PYD.wn)..........]...>..t...k{.nk.>..y...n...S........{Dc!H._.=JE1.@28..a..wRH.!......{..G

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\img5[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, baseline, precision 8, 50x50, frames 3
Category:	downloaded
Size (bytes):	2037
Entropy (8bit):	7.719074917039759
Encrypted:	false
SSDEEP:	24:jnWp/jh1UtqprLlE78F3kR6T9VVdL7qlghl5sexXO6EZXb1YVt06Hg7/tYqVFCdS:D2Ds760S9VV9cgz53o120sg7HVFIEn
MD5:	6D02D5CF49120718501B9A6629290C48
SHA1:	A7BFDE16CD37F6A331E8F17FBFC2F1772A5929A1
SHA-256:	84D7F0648AEBA8D80BB0F47E781CBA8955B8FA7425748D9830C7A8C9BC35E5E9
SHA-512:	18ADE57A6DFCA345F39807CC19B574783B7BF3B96042F47543F03F2EA80845B7965049AE6E1F9E203E54E1F3692F44C842822AA62186A607B5D6037932CFDD75
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/de/wap/mobsurvey/img5.jpg
Preview:	.....C..C...2.2.."......................................<...........................!..."1AQa2Bq.#3R.......Cbcr.. ....0........................!.1A.a..2Qq.....$4S..............?.Y8W._8q...4.M.B.H..8....V........p..\$.G....F.J...CN....!.3L.}.k.A.!a%..........9..xW..P..&EMn=%.]Jh. }l. ...Y........%.6....w...~.E..&.gT....E...$s.t..d...jR.%X.9..L3.A.....u.n...F..EZ.a..]..(..z..GF.F......}a..9.U$.T*\$...*ZF.................-]k:M...l?P}.=d...J.C..k..7_n.F(~...w...^..s\|.Vg...bz)....e.. .m .....I...."..MT.)K%..FH...Jl.2...f...q....F#)..\e!7S....o.O.7S.....s.T<..kB`F..........p..[...v.<3.z.z.#'V.2).wes..w...J...<-.!.W$d...r.t.6.t...O..:.jl).b.V...........@....h.#.J.bA=.............,.. 3..!.z.H..Ji...5&">..T....H.=....V\.0.h....Y...L.=.W46.......i*C.)K.@.J.(..K.<jU{1dx9<.*.j.....3b8...>t....Q....j#<JV...^

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\img6[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, baseline, precision 8, 50x50, frames 3
Category:	downloaded
Size (bytes):	2143
Entropy (8bit):	7.729942906424524
Encrypted:	false
SSDEEP:	48:DoHwzmJpXz6r3IfAVoh2j6SMwLzFMneoKPpLUTF3af8sWux:DGwzmOIIKO6ILzGneoKPpLoFqfEux
MD5:	F48AA7778890400E3BE6131E64CD4236
SHA1:	9341D039B9F7DE4EAC9070C36FECAC2772CC1BA0
SHA-256:	388E1EB0CB648490EA1C4913F4EA3128F3FBFBDA0608BF85E471D947DB905302
SHA-512:	11D25FAECD0591BC929571746CA56C3BEDCC5AC951248B123EB948B5DFEFA6C0CF2F6E841F8681BA5B9E9165343DE4072FC78F71832E515D464DAA2E849C84 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/de/wap/mobsurvey/img6.jpg
Preview:	.....C..C...2.2.."......................................@...........................!.."1A.2Qaq#%3..... ..$45BDRTbcdrs...............................1.......................!..1.AQa.."34.....#2Rq.............?.~ .!..7R). .1.#.......>!..N[q.Sq...=.rz .2..l.G.Fz`..K....)...0.%.'..2.~...w_z6.-...{.v5D..Z .y..]h..K..lTH....N..........\..WRe...\..f.!.Lf.....{.mH'....r:..O.;..4....R*v..!.`G.;Ky*..L.Xu..$aim...(..5....@......`..WU.6.Y...{g..:.-...p...N\J......7<O..O....j...?Z...J..R9T..*>....9..yj..qe..+H $..,.2 39"6...K*...f...z#.>..o......T..q]I.P*$.rI9:y..3..;{xp.]...(....,.L.^[T.M%Ii...%.:G..M'.shY....5...L..E.....x..[...........;..WkVw..7UbS...A.[.G$..R.....$s/..bH.P.NGs.\K..KpLq.:N..... N.$..O..N...>.O...;.....n..h.sU..]....?j.ip...u(_..8?0tkWI.........:K..Vd..#.b.R...X..}.....+..+.....k*.......<.Z.%)+..O0...C.V.I.&...S.X`z%..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	86659
Entropy (8bit):	5.36781915816204
Encrypted:	false
SSDEEP:	1536:YNhEyjjTikEJO4edXXe9J578go6MWX2xkj8e4c4j2ll2AckaXEP6n15HZ+FhFcQ7:uxc2yjx4j2uX/kcQDU8Cu9
MD5:	C9F5AEECA3AD37BF2AA006139B935F0A
SHA1:	1055018C28AB41087EF9CCEFE411606893DABEA2
SHA-256:	87083882CC6015984EB0411A99D3981817F5DC5C90BA24F0940420C5548D82DE
SHA-512:	DCFF2B5C2B8625D3593A7531FF4DDCD633939CC9F7ACFEB79C18A9E6038FDAA99487960075502F159D44F902D965B0B5AED32B41BFA66A1DC07D85B5D5152B 8
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\jquery.min[1].js	
Reputation:	low
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/3.2.1/jquery.min.js
Preview:	/*! jQuery v3.2.1 | (c) JS Foundation and other contributors | jquery.org/license */!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.2.1",r=function(a,b){return new r.fn.init(a,b)},s=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,t=/^-ms-/,u=/-([a-z])/g,v=function(a,b){return b.toUpperCase()};r.fn=r.prototype={jquery:q,constructor:r,length:0,toArray:function(){return f.call(this)},get:function(a){return null==a?f.call(this):a<0?this[a+this.length]:this[a]},pushStack:function(a){var

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\returnDate.de[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text
Category:	downloaded
Size (bytes):	1257
Entropy (8bit):	4.66897000456621
Encrypted:	false
SSDEEP:	24:XEY0MYIh7ggLKYgSA9eY9JhDqjxPrVcl6Rm/DG5mBtqRmBBQmndyAlCw:XvCL3hErul6Rm/+mBtqRmBBQmndy8Cw
MD5:	50C340711D920FD7555736D4F63B227A
SHA1:	0ADD481C5A8FBEA2997036DE8093D4F079CBC335
SHA-256:	F7A34F1C806BB9C1091558719CA37AE42B7489B3742C67DD850F177B1D635A45
SHA-512:	AB0AB02E2081DFB7862AD04EF2966D348B5D14C4219983BFEDCEE4626BE68B16521C780867D2BB2927B119A61304AB510AD65E4ECAE5971E6B86207655EDBA30
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/de/wap/mobsurvey/returnDate.de.js
Preview:	//----------.//----------.//-------- GERMAN DATE CODE ----------.//----------.//----------. .function returnDate(format, print){..var out;. . var curDate = new Date();. var year = curDate.getFullYear();. var month = curDate.getMonth();. var day = curDate.getDate();. var dayofweek = curDate.getDay();. var hour = curDate.getHours();. . var daysofweek = new Array('Sonntag','Montag','Dienstag','Mittwoch','Donnerstag','Freitag','Samstag');. var months = new Array('Januar', 'Februar', 'M.rz', 'April', 'Mai', 'Juni', 'Juli', 'August', 'September', 'Oktober', 'November', 'Dezember');. . if(format == "timeofday"){. if (hour < 12) out = "morgen";. else if (hour < 17) out = "nachmittag";. else out = "nacht";. }. else if(format == "dayofweek"){. out = daysofweek[dayofweek];. }. else if(format == "day"){. out =

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\LKJTJ3TX.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	56261
Entropy (8bit):	5.943165934486077
Encrypted:	false
SSDEEP:	768:SCYR49z3ZNh0cvpUBBbxN/phgCyefIshKijXyuFM9wCD6SEFVi:SCl9bfrxUfbxNJfInuqdEFVi
MD5:	E5EA140EC016DA33D1F20049AB950544
SHA1:	714DF4B4027FC02757032E21BC713BD18EA3568D
SHA-256:	96EFA63EE0303B21E86EF10E61FA32223D99A66CAA54147A34DE1A94D8B967B5
SHA-512:	5DAC82A94701C8A62CF398577559C2B80F9490E86342BD8EE3FE2ED01E08FD632A33D9F1991C7C138442D2DB32B154A7CD0D04BE23C4AAE24AD24FB6E1F34EB
Malicious:	false
Reputation:	low
IE Cache URL:	http://prize-winner-ko3d.live/?u=1nup806&o=0wywy2l&t=k2Dr
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">..<html xmlns="http://www.w3.org/1999/xhtml">..<head><script>function requestLink(){return { sessionId:['sid','t4~xrile5icp0uydarybx1kpaml'],p1:['','https://wondertrouble498goal.live/lyxrxqcy/'],jsFpCryptoKey:['','q8efz1cg6dcbq4e0'] };}</script>...<title></title>...<meta name="viewport" content="width=320,initial-scale=1"/>..</head>..<body>..<iframe style="width:5; height:5; display:block; visibility:hidden" id="frmin" src="/media/mainstream/frame.html"></iframe>.. .. Loading ..<script type="text/javascript">..//38..var CryptoJS=CryptoJS||function(f){var r=Object.create||function(t){var e;return i.prototype=t,e=new i,i.prototype=null,e};function i(){}var t={},e=t.lib={},n=e.Base={extend:function(t){var e=r(this);return t&&e.mixIn(t),e.hasOwnProperty("init")&&this.init!==e.init||(e.init=function(){e.$super.init.apply(this,arguments)}),(e.init.prototype=e)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\bootstrap-mini[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	10214
Entropy (8bit):	4.93220420104512
Encrypted:	false
SSDEEP:	192:f/FOG/K0sNKSFVhc6iuciuM5Kv4HvFBbLQ3X67Fayq2:n6LQ3X6Zay9
MD5:	F0A842B8B8A52BB05E6C729828FBB40E
SHA1:	F1FE8A76DB92BC9BD3F9D70F3867F03D51EBBAE5
SHA-256:	EB9FE798331B592BD8FC54D5EDE3AC19E961B5AA7C2DFFB3DBB17CE5FCB88E01

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\bootstrap-mini[1].css	
SHA-512:	E1CD3AEED619702D22B080FA17488267DD24287B3390C6DF0624E6D51EE28D53FC340C5A1E213E1A98EA40611C0545B9BF9B5E5EA8FD22D4CAB9E2297ADF748
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/us/wap/mobsurvey/bootstrap-mini.css
Preview:	html {.. font-family: sans-serif;.. -ms-text-size-adjust: 100%;.. -webkit-text-size-adjust: 100%..}....body {.. margin: 0..}....audio,canvas,progress,video {.. display: inline-block;.. vertical-align: baseline..}..a {.. background: 0 0..}..a:active,a:hover {.. outline: 0..}..b,strong {.. font-weight: 700..}..img {.. border: 0..}..button,input,optgroup,select,textarea {.. color: inherit;.. font: inherit;.. margin: 0..}....button {.. overflow: visible..}....button,select {.. text-transform: none..}....button,html input[type=button],input[type=reset],input[type=submit] {.. -webkit-appearance: button;.. cursor: pointer..}..input {.. line-height: normal..}....table {.. border-collapse: collapse;.. border-spacing: 0..}....td,th {.. padding: 0..}..* {.. -webkit-box-sizing: border-box;.. -moz-box-sizing: border-box;.. box-sizing: border-box..}....:before,:after {.. -webkit-box-sizing: border-box;.. -moz-box-sizing: b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\facebook-icons2[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 23 x 766, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	5786
Entropy (8bit):	7.933833715102447
Encrypted:	false
SSDEEP:	96:Pg0oFs7A+jETZfzCR79eXWiDSz27B5EZGUhL1/HFedxpWKMCfyg:Pg67A+ATZfzCRJeXWij5oRxMxiayg
MD5:	EE2E95C6D88BF77C809F0C65DAFA34E2
SHA1:	119233DF6BF224B41BC59ED1BBFA34F9BED73BB7
SHA-256:	EFA8D9BBD0AFE26B0ED378E4FCB204738D96085699EAE4BAA7058109F4FE5E2C
SHA-512:	ABE98C062122B398CEC7429A995EF77B201B25C77CC86E98EC11873683D9980F738E2091D9AAF53090D19526B5E8B78716C948CE64F343CE71400C227B7894A9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/us/wap/mobsurvey/facebook-icons2.png
Preview:	.PNG.....IHDR.....q .....PLTE.....r....x...rM.....r.....r..r.Ui...Pu...r.Ug..s.....Ti@....r@....r.....r.....hYL.....r.....A.....I..>...gYI.....9X..I\....h:X....A..en.....[i.z....U.....}0..r....v.6U...r.Rh..W.....:X..Wi..r.KYD....V...?..:X....J.vX....r=}..##X...~/...zc..o.....G.....qS.6zc..ReG....L.....o..mzc.K.a.....I.....B.....h.Dzc...ov.....iK.\.....r..[..]K.i.,,..r..r@.....RhX..e.....&,8.....lK.]....:..I.|.{e.....q.....35<.3.sj.....m..n;Y.....^i.g..p..m..XA@?..q..k.hj....d.aOKC..T...\ocK..o~rO[TFH....n.....,_....i...i...0.....dx.....v.1.....a.wX...gz.n.Q.....i.ad^H.y..GZ.XP...I.....lY6D4.....tRNS.....1....\.;*.q...@...p..P.kP-.....et.<PM*.q="..a..qA*..gb^.-&.....]..... `,.....P&.....~.....ID ATx...o.a..f.....".hH..UUG.!..~.W..-q.._v..vv.m.].[].(.m....EU.n!.%.w.y.=.2.....y..}.gf.....k....6...1...|-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\ie[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 245 x 241, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	3784
Entropy (8bit):	7.891528024698781
Encrypted:	false
SSDEEP:	96:9zJx6uOhFbpK9yrP1tp4lklAyancO/+DFLV6ptS:9dx6rhFbworP1tSlbRcFL8tS
MD5:	A0DB15B639D5375161EF299FC22A9E6D
SHA1:	5FEA3A9E67EDB6F8A1A5EE6D99E259DD83AFF686
SHA-256:	DD21E3489A111B59404CDA401A90BDD74331500B3B8C4497A0F288D2CCA830E7
SHA-512:	88C7D39A7ACB0DC3624C3348D9CF58B4486BD70DC78487B2404163F0D1C085CB6E02E709BB588D634B14437EC4175CEC5CA3A416669E36AD095749E9B97E637
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/us/wap/mobsurvey/ie.png
Preview:	.PNG.....IHDR.....$..A....PLTE.....V.....3tRNS..i.....z._..@.'..;."..F1,....6s.Te...Yn.KP..O.....IDATx...Y{.P...9.#....(n.....k.1.....$.{..\8..3s.....'K..T..h.~o4.W..3..Y.....N..kR.....D.o..n.Vq_..E..{g....bo;..._o.."....>?-^g....[.>...`..W..gev...9.`B.P.....wn....}&.....E.D.h..%.}..G-.eZ.?lm.E.V..M.L.@^.s=l.c.<N=W....=..h.q..C.....Y.E.p\..1..V.1.~.7...w.|.[.....]1itC.w..R..7.;N6...C.3...n.w9.t..&..O.,H..2....Y3.g.=.....n..H....}Cw.....#Ai.....ks.M..c9.j$n.....=.....J.Doa.....].%.H..f.WIF..K8..='..zK.....RA...Q^..?(.Um2s9*.. .....V....P.n.9.M...CU.....G./...c.]T.....Xq.w.f.J.....)U.....+.....JI.!.).[$...R.....S0...:u8....DjWEQ.C...8._..\..%.,.<.4.....:.r.v....U....`:*.j.....H....r.<.=...!..Py&G..K...=.....Oe.....M'.@hRI.....*....*.3C.0[.....6t..lK

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\img10[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 48x48, frames 3
Category:	downloaded
Size (bytes):	1506
Entropy (8bit):	7.601187549360118
Encrypted:	false
SSDEEP:	24:995kg71mT8EdrvlDrfUVYN/u3IladQJz9iwaoo7/pFY0YfCmtI9vi02N:H59mYEdrZMSN6NUcoorpHYL0MN
MD5:	0D0F29ABFCEDC7DFFFE3811A5100A6CD
SHA1:	19567E85AAB4FD05D752CFA86F88087465042B0A
SHA-256:	E3DA7D20BE42DA6E260D3085D2A3F3965A549065345EE2D139E28625104E2393
SHA-512:	9F7465AC12B6C5C803249FF65650B51D6D1B13C316374E0869B489D8D9C48C63F802E8C282603D20A2208B9173D400AB955CE529FF46242282F9E97A58FD3365

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\img10[1].jpg	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/de/wap/mobsurvey/img10.jpg
Preview:	......JFIF.....H.H.....C.....C.....0.0..".....4.....!..."1A ..2Qa.#Bq.....3.....&.....!1.Aq..."B.....?...a.U..2H....?\tE=...\...F....|..)..Gb\..R.....c.T...`...{....c.....S..=&p....Q7)..df.]..?...0V.kZp.%.....NI #.....%.....6.=W;....j.sJ.(.u.t.....!..e'....H.....kN..>..zY.z.5....e.,2F.Q.G..e...+.R.6#..e.t[E.X...w....~.},t>wX..%L..H.UK...NT6*v....Gc..l.2.nu,V.+([.....S....~....4.....UN....<....#.3..<....9H...../.....V.G5.m..p..D...U..h....+....o.Jj..i..".P.....D...8pk.G..U.K.iMA~z...>..I"..~....S.:z....5...t.....Y..,H$..=..ljrP.@$..=:.....J...].)Dn>./..N.[)e....q..cH.\.-...:F...(iCC....:..... .S.....m..O.`.sG..0A,9M,.v..T.S.....av._.iz..TI....0M..Dxj.{2....q|..... N...G.2..e.c.PO..v...=rc2e.E..!../..F#!.v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\img1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 50x50, frames 3
Category:	downloaded
Size (bytes):	1315
Entropy (8bit):	7.494283416166172
Encrypted:	false
SSDEEP:	24:s/rPxB67VxGLIAKM8gWos/HcF9UiHjlY/BSEPDtU8CA:s/bxYkUXgWD/8D/Y/B5PJU8H
MD5:	C3C59916D3B4977017C89125DC42B664
SHA1:	C8E5A97A6E9FBF41558C09C65B2CA6DF9BA8723A
SHA-256:	AA05DE326A8AFD2A7B16C253D8C10FC41857B474F23A814FFA7684D4EF17C1A9
SHA-512:	489B210B049F032D63A0088E2387AAF160AD57210B89EBE25D6E1403913CDDCFACDCB122A0C92B7877B6D7F79D3DD2B96074894E1F3CBA283EA8392612E7756
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/de/wap/mobsurvey/img1.jpg
Preview:	......JFIF.....H.H.....C.....'!..%..."."%()+,+. /3/*2'*+*...C.....*...**********.....2.2.....=..... .....!1AQ.q"Ba...#$5s....236CSTbr.....!"1.A.....?..M.lg..JyJqCx.xBF}a...s\.N..H.h_....N..B...^FE.....\%..j..t.))-. g...r...>2.6....C..>.. .....e.y.i!.PeWtn..o.R.....&.....7..... .`..a.'3...>..h..g...HIl{Cm.z.....-.....2...DV...P.v.Ez.....2.w.`.zJ7...`...]{.Z...9.o..M..l....5..9...P=~.K.....=..S.G$!c.d..M{..x...6...b....!)ul7. `.$..g..iR.....w,.%l."].1.iu.8...)H.I..>.)D.....3v&..M%.8..\....W*A....{Ep."....BY.ie.p\'*<k...h...i..@..* z ..dg.E....C..SfYd.....)u..w..x.C.Z.h.....U....r:.J[p.....<.....7..". ...w.[^.ou.<I...u <.O<.....E.[..k..]......].....tv..M.O.9rf...AW..\.....y..5b.\.b...2.}...Q.."A.H.Qd.....vb.8.9.....rH*...P....$...JnE.....I...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\iphone11pro[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 300 x 402, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	35991
Entropy (8bit):	7.981976976434473
Encrypted:	false
SSDEEP:	768:4pH0R0R0UJviCBq/FqPSeVk3b8JdMJky2L3vXw6lEz245u36To0sPfpwpWJhA:4pHnXvi8PS0uUqJky2L3vXWB566To0si
MD5:	80311B6F5B7AF08899350D4DCCE87EE6
SHA1:	B4B9A1B3A777AAAEB0A19866B743D6D3BA861A5B
SHA-256:	BD1C43C51E6D8B7669315F6A44009A78B5D6542625AFF8F6136411587F600493
SHA-512:	D3907E77E34FFBB3903BE47CC59691E524BBC4F76D0B4698A3F793E23EED4E3567768AC7E0864E627D5AE4CE79AE1F9B6511A5A37D4D22C607EAEA99913D446 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/us/wap/mobsurvey/iphone11pro.png
Preview:	.PNG.....IHDR...,.....nc.B....PLTE...PPO(()...==<%%%..../-<<<ffe777kki...DDBQQQ777/////....""""000"'555...ppk.....PPP... 222.....iii.....'$-4!*1...555.$+...'.....&/7..&."(.....(19....."....%)4<...8O]...IIH."*.. ,>H7HS...0AK.(07LX);F...-BO8882EO+5>LML...!/7/;E(8A$2;[\[...0ET;Sc...$4?...E` q.....2IW2>H-9BddcXXX.,4AXf.%....<<<...UUT-7@.....Mgy6BM...^w.Us....s..b..Kds%7C...@[k.....sutp..nom...Qk};[r]{.Df~||ya{....u..:Vj?Q\Zs.|..Z}.Uo.y..a.....F]k=KVl.....Uy. [w.(>LDDDl..f...*5...@Ua.....@@@...Rq.%%%.....h..?`yf..Fcxz..1K].0<...o..RRRz..i.....)...5Pc``_*++.....n..JMS. /Mn.Mk.....Ss.u..Gl.....Lg...#lV_...8?H.)8T{.\bc?FO. #7t..P_i%HU.-A...Xiu+Ve....7H.....,_.@}*X..B.APn.<....+.d9....tRNS.M)....O.b...<z.....K....7I....1IDATx...o.T...%..].(P.e.J.\..Z.."J...@...5.(<P0K...{!M|5<HbBj.>...K\`/../j... /.....8....i{Nw.>..~...]....._..?.[n...[..F.;.z....ez.a.W...[o..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\logo2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	11192
Entropy (8bit):	5.809682664340976
Encrypted:	false
SSDEEP:	192:jFUjeecGUUMwa8skoVjjrV2+xWRnENAZv/6XWXVsL2IFv3N0zEHh9l02+6Tf65Jb:jCj8UM10o9g+xWuCZv/6mXVoN3Nnh9lO
MD5:	C1BD16B2E39C5928B80710D02238A99F
SHA1:	D74EFD774B1FBBCEF95DCEBD8F2E33C1788E2C94
SHA-256:	14858ED060AA807E826E006A44E5812742A3AAAC775BD27209CAC463A9C19EE0
SHA-512:	F99113DFFE1A830E9538A84E3C2D1FC653C4562378670CB6BBA027C5BC709DBCC07EFDD90DB48EF76A4F020A4AC996F6C8998F19FFE741DB7371B62C91FC34 2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\logo2[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/us/wap/mobsurvey/logo2.js
Preview:	var a=['L3czw4DDgzI=','ZMKzH8Ki','w4nDpMKA','wrPChsOYwqTDnE5NG8KFw7htw6A=','w7zDv8KRw7rClcOowoU=','F8OdSG8Lw6QmwojCtsKVJ8KMwpRS','w4vDp8Oh','NTPDjmBFIg==','bMOhEMOeY3NOUH3CtsKNNTFxU8K3WjbDj8ObXcKsFMKKw45iFMKLTcO1wpsuIiYAwqU7w5bCmlYd','w58cwp/CmA==','w7zCv2oc','CShSw4FEF8KaDMOYB8OP','ZsKOw6MwQ8KYwqo=','w6Aiwqd3Ci91','GMKaP2nCiTIjQG4swqFgaVog','woZnEMKoIMK6Ag==','w6TCoV8YcgU=','wrJww5xoccOk','PMKQKAzCpjgtBUIqwoxuU1s=','GcK6wqY/LMKqEQ==','wpjCrVwdaQ3DkjzDnHvDqBLCpRDDj8KpaMO6wpjDl8O0w5nDowcswrLDtsKsGWXCkh0bw6jCmF7CssK0dhPCq8OhfsKZw5dbw45+w5I=','NCs5GsKmw5HDrcOLwrDCp8O/RsOowoI=','w5MZw5JUwrRQ','w4zDp8KowoAQw51iAMOmwrTChhVQF3zCugIvPCAew7ZoWsKuw5fCkwvDgcOTWMOcwqXCnC8iw6M1AMKNdz5ieMO+wq3Cuik=','IyBTw5BrFsKG','BMO7w5FuCMOFw4I=','wpZ8w4V7fMK5KQ==','QsO4w5BvGcOrwovChMK+XsOwwqvDpMOzQHjCgSzCgsOANlMgwr8aMQUWC8KHIsOdw6pjHnbCqsOMwojDicKL','DCdFw5B1NsKY','fcKxw58=','wq9IKMOlHw==','w5ZSw7Q=','OzvDm0JMdcKHwolpXcKZBk7Dsg==','wqhvw54=','w5TCp8KwwofDvHM=','wqvDhDDCiAvCjmnDiMOiwptbworCp8KDQxE9w4fDuQFLw5fCnsO

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\logo_f01[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 130 x 126, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	6763
Entropy (8bit):	7.888794921730071
Encrypted:	false
SSDEEP:	192:Pifv2RWvggJqE+ZNTZRh/z7W6nFi1aCpz4/rT:mzYyqE+ZHRhL7FnF3GMrT
MD5:	192B810BA6ED4B80611AEF274D85948D
SHA1:	2835CC503EFCD77D03613293DBC33C4CC7B6B5B9
SHA-256:	91E5C1968EEE9298437A097FD47978A077D667E086593AB0FD7988EF60D2DDF4
SHA-512:	37E35537391AC2FCDCCB027761089ACBEF1E1DE3AB6E77000096D75B5487185705E403D8BE7AA1123D000C3A93F46808B2FE89D854633957B3A67BC914EFAE3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/media/mainstream/de/wap/mobsurvey/logo_f01.png
Preview:	.PNG.....IHDR.....~.....9.....PLTE.....E}....7j...+....h../.-f..2.,Z.....7s..-.#V.O..!.D...(Z.o..o..n..e./.....0..p.c.....G..M..$..q.....l..)^...}..... ..wk..... ....>..8.....E.....K..3....$Xg.....0l.,eo...~..[..... Q.P.....(^z.....n.....U.`....9r..B....i....[..E....J..3j.....e..I..<}.....u..M...t..5s...X.....R...y.?z.....B.....`.-`.t..U.....3..)..... .....L.....0...C.....=..6.:.....v.F..#..N.....}...d.....l.b..U.....U.....\...'V..~.Y.....n.....k....k...a.....S..H.t.....9...}..@..P....+ L....4..H...Q....3|..^....$j.!Au...;..&...~TLS.... ..!..K/6^...s....s@Bp..P-.E....<...}.b.u5o..U.....rpz."Kb..<...L!.....eQ.PAd,;.s.~..Uc~.yt/*B..>.]....gX.~..9..t/.....;tRNS.....,$<I3Wl`.....x.Z...~..@)....~@.....u[[.0..... e....IDATx..[L.g...q.l.l.....s..;..].J=.V+.B..-.v-B.@km.....D..X.).X..@.K....b..JX:0h.@".m.1q.....-.?.x.....X..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\lyxrxqcy[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text
Category:	downloaded
Size (bytes):	17177
Entropy (8bit):	5.049648953907505
Encrypted:	false
SSDEEP:	384:U6ZLF0eWHAIHuIJ5ECMvZgY/mexVklKPImuho9HGUBGUsBGUEGUoGU+GUesGUiSy:DngY/NG9SVsYKJ1
MD5:	885138A6D6DFDA6E4A40CB7BC03DA6F7
SHA1:	413D8DCCECEC7D29512E825B5052B8D63FECF688
SHA-256:	1EF9814555CD97DDC1FFAAA6A49A829F21F068D563AB2B6EB2F34FE329B0697B
SHA-512:	D2926B06281616FB9798B9B343073C52A12F864FB9159E4D18C9D6DD0AB7EF5460ECBB23BB65BD55E6D0B355044594F5ABC282959E00CA500C58BE5911A741D
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_31, Description: Yara detected HtmlPhish_31, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\lyxrxqcy[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://wondertrouble498goal.live/lyxrxqcy/?u=1nup806&o=0wywy2l&t=k2Dr&f=1&sid=t4~xrile5icp0uydarybx1kpaml&fp=QiwVEmmXGLT%2F4VyjuL01JlaZrE51HANMduCGylmuvr5qkBGvk754vCdZIMslGa8OiwWsMrw4ylT76YJ65x3UXe%2BOHSpSCH4T03uo%2Fpcao76x5KTig689s%2BlhRvvZXX4yWFJWVsZZxVbha8rv8iUo6fdKs1WyTr4GcSuo3jReGssiB0Qml%2FQgpO9UgE9jUQJ5NWd9DTpBwkUI1fucYBSSqsG8b%2FdNSz2w%2BlNb4qZAvksAAfyy0z%2BncCaOKy%2FQ%2BBm5qq%2BIMW4iKoJ5dr7%2F5CeJrF5fMWYRpTbumjUFdDKNbUhxU8FPe0UBr4PHJPHIvzIzTTCluZGi%2Fei%2FiSQcziVHUyzWYk2MTdcvVAACg1nTXu1fwFnnjpzMlIJsSGr5d1Gg2o2RyJ15MvHAFKlnQe%2BWMWCeI4WYmohlCbWetpflaU6Ml4rH3hneZhhZxgNq1VCWSMGnC%2FlulNeQhAA9chlXvowTXe%2BhTx9wt4PW34XmljSlFhckMm0MDvcBxi38hyV671VpndAsa2jujLUTlhZowqotBDkvxn1kf7g4yiCb%2FrSxVxBXkEinBqxgJd%2Fm47xSKKHV6ctwpNce0xH0IEjheQreZrRQKdjy0mex5iGz7CxxWgUBLbc1Onm7BttbaX%2FB50x2X%2Bu9XwDImj0CSjDuu46116gm8rzoksKJJZvPbSpQxi%2F8uF3tIXK%2FpxdzdFjVX9P9EWao4TZJ5rdU%2F30eEHhoMYUxQi9dJ%2FPIzaMtnDROic4zcEgqRheRQDX%2F9vLmYBXe2bVYueesFdJSdiR%2FFU31acJY7ZGRWJQOuHTIoUiJ%2B10yMdeyJ%2F9K6Gti6Osqu1AJA4CdTft7Z9iw99UWazK08K8pUm4xtkfvtBz4lA6jvu4pJMoiMgTlpftVQnhpCyWu83zJJlIJj0yD%2B%2B%2BJtq84XaNibyIzNtZg%2BSVgMNxlMw8cI9mt9n4sTPEYecII5GYNJ7SCQy%2FvRsgrWEttUWPSVJqPAmbXyj4tyjXYyFy%2F4sH0LREFhYHrT2SkXYFPt7Y7XAgh3Lgmy3t0jpuENSaD%2BVuQuVdQEGDEk36F4u1a1aLqADVDc8gDnkkOd33HtPLxthbXOxal3t5eHYRYQM3v%2B5E%2FeN8F7h2t1rHuPKlacRclzSO7wMQbhVYK2bCIAMAg%2BdrlALmPoDonr2nlyUBNANSPgRROB8QJOM81ydfQBbDpt27x%2BycHRx6FfkzViO7Hp0ITaAyiyhtLhutIFaPiD9s9hqV9LqiZjAbZ48q2j6YI0cvEPqsxoqzKt2nXPHSIxYfS8iTRaI330fGsOu7%2FGta18hm3h4P5oBSnjZ6yTCMSGUsO%2FvaXTpf6WXXvq8OjqPeWc3Oy6YtQ9I1PBoomK9JOtlV9mZ5Nws95Y4k1WzEbiNC0f1ocXRrDITp7
Preview:	.<!DOCTYPE html>.<html>.<head><script>function requestLink(){return { sessionId:['sid','t4~xrile5icp0uydarybx1kpaml'] };}</script>.. 453238 -->...<title>J.hrliche Besu cherumfrage 2021</title>..<meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>..<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">..<link rel="stylesheet" href="/media/mainstream/us/wap/mobsurvey/bootstrap-mini.css" type="text/css">..<link href="/media/mainstream/us/wap/mobsurvey/font-awesome-mini.css" rel="stylesheet" type="text/css">..<link rel="stylesheet" href="/media/mainstream/us/wap/mobsurvey/main-like.css" type="text/css">..<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.2.1/jquery.min.js"></script>..<script src='/media/mainstream/de/wap/mobsurvey/de-en.js'></script>....<meta name="robots" content="noindex, nofollow"/>...<script src='/media/mainstream/de/wap/mobsurvey/returnDate.de.js'></script>..<script type="text/javascript" src="/util/utils-

C:\Users\user\AppData\Local\Temp\~DF2F2006B451AD575F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.48231359819970593
Encrypted:	false
SSDEEP:	48:kBqoI+ZS+ZM+ZFZvZGv6ZiZvZGJRZqZGJRZQZ1NiZ1N2:kBqoIBHjgH+
MD5:	FBA8E3676BF5615C0137F851F9F0245A
SHA1:	73EBC40EDA148B7586132A38CDFC02BDBBCCB2F7
SHA-256:	852447A5E7894FCD1C7FBA407EE6D3E7413EF683D62F9CD458A0E59D679EA008
SHA-512:	702123E5F8F52BCB8AE15F1BF12B6714DE7288150767504B120448D98ADFF8D682E454933845A8FDDC4C737432DDAB885E1C5FB5E1BA784A3D1741A51D3419FD
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF42082C2DDAC0DDAF.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.3691232092148859
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAIBhS2XV6LE:kBqoxxJhHWSVSEabqV6L
MD5:	3E82D84677908170AB65E4463DAEBB35
SHA1:	D948E2FD7F8366C3AF7D7200F2630625404CD7BC
SHA-256:	B1CE734B146A8B9C89D8B3598F2951702E4A5EABF31AB6F6C5613CF9339F022C
SHA-512:	12E2045A7C85F1CB7F747A0081328555F0E1F48774A4C11853D415B834CD8C680EA7157BC826628EFDF93B01224E8BD3BFE794671BAD93905075DA2014B2D003
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

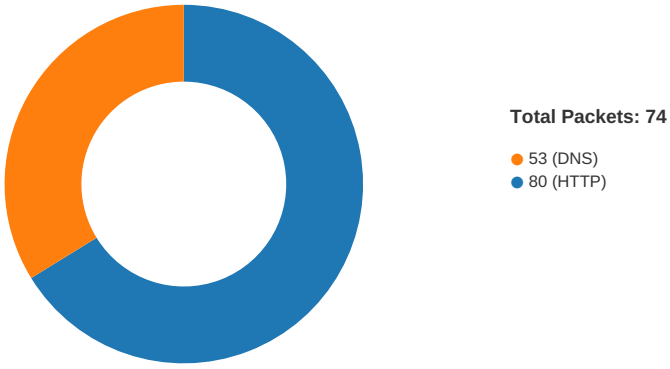
C:\Users\user\AppData\Local\Temp\~DFB51B924042DA2D2E.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	149344
Entropy (8bit):	3.0666453028890874
Encrypted:	false
SSDEEP:	1536:1ZhjZ+jZTZ1ZhZYZmZXZDZDZDZDZDZDZDZDZnZ7ZtZ0ZzZkZaZ7ZHZuZc:zhF+F1zPEeJllllllllZdrwVgid5mc
MD5:	4D2892CD200FEAE343D0A3C32FA9BA92
SHA1:	2A51CA8ECC7E0B8FFBEC6B802B0E7140937648E2
SHA-256:	235F659E6109EB0C171C63039296CFCAC55D624F8A419479AAA2A766707DF0E5
SHA-512:	97A6C318303709560446C2D71961BF7CEB351B0C0B670A001ADEA8C5CD373C20E3D773D468A714E7D2317805DD95D659BB6830E4CE22F8A1AEEED385D3B5795
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
Mar 5, 2021 10:10:12.230678082 CET	49683	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.230681896 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.282732964 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.282782078 CET	80	49683	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.282906055 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.283024073 CET	49683	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.283524036 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.335391998 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.379520893 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.379584074 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.379661083 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.379690886 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.379714012 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.379754066 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.379756927 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.379765034 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.379791021 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.379829884 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.379848957 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.379869938 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.379897118 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.379919052 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.379935026 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.379966021 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.380006075 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.432140112 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.432203054 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.432245016 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.432266951 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.432282925 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.432291985 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.432322025 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.432332039 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.432358980 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.432362080 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.432404041 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.432405949 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.432449102 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.432451963 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.432487011 CET	80	49684	5.8.47.58	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 10:10:12.432492018 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.432524920 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.432531118 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.432563066 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.432571888 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.432600021 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.432619095 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.432636976 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.432637930 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.432674885 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.432686090 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.432723045 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.432763100 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.432765007 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.432782888 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.432801962 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.432832956 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.432838917 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.432854891 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.432879925 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.432907104 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.432934999 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.432967901 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.433012962 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.484741926 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.484920979 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.485029936 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.485073090 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.485110998 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.485114098 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.485129118 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.485151052 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.485168934 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.485198975 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.485205889 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.485240936 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.485255957 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.485276937 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.485316038 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.485318899 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.485326052 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.485352993 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.485371113 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.485423088 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.485433102 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.485465050 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.485502005 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.485539913 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.485541105 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.485548019 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.485555887 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.485586882 CET	80	49684	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.485594988 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.485642910 CET	49684	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.516791105 CET	49683	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.570631981 CET	80	49683	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.570677996 CET	80	49683	5.8.47.58	192.168.2.3
Mar 5, 2021 10:10:12.570774078 CET	49683	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.628387928 CET	49683	80	192.168.2.3	5.8.47.58
Mar 5, 2021 10:10:12.721158981 CET	80	49683	5.8.47.58	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 10:10:11.075253963 CET	61328	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:11.134325981 CET	53	61328	8.8.8.8	192.168.2.3
Mar 5, 2021 10:10:12.174385071 CET	54130	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:12.220859051 CET	53	54130	8.8.8.8	192.168.2.3
Mar 5, 2021 10:10:12.818651915 CET	56961	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:12.873280048 CET	53	56961	8.8.8.8	192.168.2.3
Mar 5, 2021 10:10:13.154146910 CET	59353	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:13.208445072 CET	53	59353	8.8.8.8	192.168.2.3
Mar 5, 2021 10:10:13.624034882 CET	52238	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:13.683424950 CET	53	52238	8.8.8.8	192.168.2.3
Mar 5, 2021 10:10:29.241695881 CET	49873	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:29.289968014 CET	53	49873	8.8.8.8	192.168.2.3
Mar 5, 2021 10:10:30.572019100 CET	53196	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:30.620908022 CET	53	53196	8.8.8.8	192.168.2.3
Mar 5, 2021 10:10:35.081049919 CET	56777	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:35.127087116 CET	53	56777	8.8.8.8	192.168.2.3
Mar 5, 2021 10:10:39.391804934 CET	58643	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:39.441330910 CET	53	58643	8.8.8.8	192.168.2.3
Mar 5, 2021 10:10:40.659708977 CET	60985	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:40.705593109 CET	53	60985	8.8.8.8	192.168.2.3
Mar 5, 2021 10:10:41.094729900 CET	50200	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:41.144737005 CET	53	50200	8.8.8.8	192.168.2.3
Mar 5, 2021 10:10:41.770328999 CET	51281	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:41.824717999 CET	53	51281	8.8.8.8	192.168.2.3
Mar 5, 2021 10:10:42.072936058 CET	49199	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:42.117353916 CET	50200	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:42.120323896 CET	53	49199	8.8.8.8	192.168.2.3
Mar 5, 2021 10:10:42.163084030 CET	53	50200	8.8.8.8	192.168.2.3
Mar 5, 2021 10:10:42.787300110 CET	51281	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:42.834379911 CET	53	51281	8.8.8.8	192.168.2.3
Mar 5, 2021 10:10:43.091152906 CET	50620	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:43.135019064 CET	50200	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:43.141032934 CET	53	50620	8.8.8.8	192.168.2.3
Mar 5, 2021 10:10:43.175344944 CET	64938	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:43.183670998 CET	53	50200	8.8.8.8	192.168.2.3
Mar 5, 2021 10:10:43.224843979 CET	53	64938	8.8.8.8	192.168.2.3
Mar 5, 2021 10:10:43.879817009 CET	51281	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:43.938163042 CET	53	51281	8.8.8.8	192.168.2.3
Mar 5, 2021 10:10:45.201097965 CET	50200	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:45.246795893 CET	53	50200	8.8.8.8	192.168.2.3
Mar 5, 2021 10:10:45.824043989 CET	60152	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:45.873307943 CET	53	60152	8.8.8.8	192.168.2.3
Mar 5, 2021 10:10:45.890634060 CET	51281	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:45.946742058 CET	53	51281	8.8.8.8	192.168.2.3
Mar 5, 2021 10:10:47.001488924 CET	57544	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:47.047245979 CET	53	57544	8.8.8.8	192.168.2.3
Mar 5, 2021 10:10:49.211252928 CET	50200	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:49.259951115 CET	53	50200	8.8.8.8	192.168.2.3
Mar 5, 2021 10:10:49.899277925 CET	51281	53	192.168.2.3	8.8.8.8
Mar 5, 2021 10:10:49.945453882 CET	53	51281	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 5, 2021 10:10:12.174385071 CET	192.168.2.3	8.8.8.8	0x3ad	Standard query (0)	prize-winner-ko3d.live	A (IP address)	IN (0x0001)
Mar 5, 2021 10:10:12.818651915 CET	192.168.2.3	8.8.8.8	0x2618	Standard query (0)	wondertrou ble498goal.live	A (IP address)	IN (0x0001)
Mar 5, 2021 10:10:13.624034882 CET	192.168.2.3	8.8.8.8	0x61ae	Standard query (0)	tdsjsext3.life	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 5, 2021 10:10:12.220859051 CET	8.8.8.8	192.168.2.3	0x3ad	No error (0)	prize-winner-ko3d.live		5.8.47.58	A (IP address)	IN (0x0001)
Mar 5, 2021 10:10:12.873280048 CET	8.8.8.8	192.168.2.3	0x2618	No error (0)	wondertrouble498goal.live		5.189.217.110	A (IP address)	IN (0x0001)
Mar 5, 2021 10:10:13.683424950 CET	8.8.8.8	192.168.2.3	0x61ae	No error (0)	tdsjsext3.life		185.50.248.46	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- prize-winner-ko3d.live

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49684	5.8.47.58	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 5, 2021 10:10:12.283524036 CET	91	OUT	GET /?u=1nup806&o=0wywy2l&t=k2Dr 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: prize-winner-ko3d.live Connection: Keep-Alive
Mar 5, 2021 10:10:12.379520893 CET	92	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 05 Mar 2021 09:10:12 GMT Content-Type: text/html Content-Length: 56261 Connection: keep-alive Cache-Control: private Set-Cookie: sid=t4~xrile5icp0uydarybx1kpaml; path=/ Set-Cookie: sid=t4~xrile5icp0uydarybx1kpaml; path=/ Set-Cookie: p1=https://wondertrouble498goal.live/lyxrxqcy/; path=/ Set-Cookie: s1=q8efz1cg6dcbq4e0; path=/ Cache-Control: no-transform Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 3c 73 63 72 69 70 74 3e 66 75 6e 63 74 69 6f 6e 20 72 65 71 75 65 73 74 4c 69 6e 6b 28 29 7b 72 65 74 75 72 6e 20 7b 20 73 65 73 73 69 6f 6e 49 64 3a 5b 27 73 69 64 27 2c 27 74 34 7e 78 72 69 6c 65 35 69 63 70 30 75 79 64 61 72 79 62 78 31 6b 70 61 6d 6c 27 5d 2c 70 31 3a 5b 27 27 2c 27 68 74 74 70 73 3a 2f 2f 77 6f 6e 64 65 72 74 72 6f 75 62 6c 65 34 39 38 67 6f 61 6c 2e 6c 69 76 65 2f 6c 79 78 72 78 71 63 79 2f 27 5d 2c 6a 73 46 70 43 72 79 70 74 6f 4b 65 79 3a 5b 27 27 2c 27 71 38 65 66 7a 31 63 67 36 64 63 62 71 34 65 30 27 5d 20 7d 3b 7d 3c 2f 73 63 72 69 70 74 3e 0d 0a 09 3c 74 69 74 6c 65 3e 3c 2f 74 69 74 6c 65 3e 0d 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 33 32 30 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 2f 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 69 66 72 61 6d 65 20 73 74 79 6c 65 3d 22 77 69 64 74 68 3a 35 3b 20 68 65 69 67 68 74 3a 35 3b 20 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 20 76 69 73 69 62 69 6c 69 74 79 3a 68 69 64 64 65 6e 22 20 69 64 3d 22 66 72 6d 69 6e 22 20 73 72 63 3d 22 2f 6d 65 64 69 61 2f 6d 61 69 6e 73 74 72 65 61 6d 2f 66 72 61 6d 65 2e 68 74 6d 6c 22 3e 3c 2f 69 66 72 61 6d 65 3e 0d 0a 3c 70 20 69 64 3d 22 64 65 6d 6f 22 3e 3c 2f 70 3e 0d 0a 3c 64 69 76 3e 4c 6f 61 64 69 6e 67 3c 2f 64 69 76 3e 0d 0a 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 0d 0a 2f 2f 33 38 0d 0a 76 61 72 20 43 72 79 70 74 6f 4a 53 3d 43 72 79 70 74 6f 4a 53 7c 7c 66 75 6e 63 74 69 6f 6e 28 66 29 7b 76 61 72 20 72 3d 4f 62 6a 65 63 74 2e 63 72 65 61 74 65 7c 7c 66 75 6e 63 74 69 6f 6e 28 74 29 7b 76 61 72 20 65 3b 72 65 74 75 72 6e 20 69 2e 70 72 6f 74 6f 74 79 70 65 3d 74 2c 65 3d 6e 65 77 20 69 2c 69 2e 70 72 6f 74 6f 74 79 70 65 3d 6e 75 6c 6c 2c 65 7d 3b 66 75 6e 63 74 69 6f 6e 20 69 28 29 7b 7d 76 61 72 20 74 3d 7b 7d 2c 65 3d 74 2e 6c 69 62 3d 7b 7d 2c 6e 3d 65 2e 42 61 73 65 3d 7b 65 78 74 65 6e 64 3a 66 75 6e 63 74 69 6f 6e 28 74 29 7b 76 61 72 20 65 3d 72 28 74 68 69 73 29 3b 72 65 74 75 72 6e 20 74 26 26 65 2e 6d 69 78 49 6e 28 74 29 2c 65 2e 68 61 73 4f 77 6e 50 72 6f 70 65 72 74 79 28 22 69 6e 69 74 22 29 26 26 74 68 69 73 2e 69 6e 69 74 21 3d 3d 65 2e 69 6e 69 74 7c 7c 28 65 2e 69 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><script>function requestLink(){return { sessionId:['sid','t4~xrile5icp0uydarybx1kpaml'],p1:['','https://wondertrouble498goal.live/lyxrxqcy/'],jsFpCryptoKey:['','q8efz1cg6dcbq4e0'] };}</script><title></title><meta name="viewport" content="width=320,initial-scale=1"/></head><body><iframe style="width:5;height:5; display:block; visibility:hidden" id="frmin" src="/media/mainstream/frame.html"></iframe> Loading <script type="text/javascript">//38var CryptoJS=CryptoJS||function(f){var r=Object.create||function(t){var e;return i.prototype=t,e=new i,i.prototype=null,e};function i(){}var t={},e=t.lib={},n=e.Base={extend:function(t){var e=r(this);return t&&e.mixIn(t),e.hasOwnProperty("init")&&this.init!==e.init||(e.i

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49683	5.8.47.58	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 5, 2021 10:10:12.516791105 CET	152	OUT	GET /media/mainstream/frame.html HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: http://prize-winner-ko3d.live/?u=1nup806&o=0wywy2l&t=k2Dr 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: prize-winner-ko3d.live Connection: Keep-Alive Cookie: sid=t4~xrile5icp0uydarybx1kpaml; p1=https://wondertrouble498goal.live/lyxrxqcy/; s1=q8efz1cg6dcbq4e0
Mar 5, 2021 10:10:12.570677996 CET	152	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 05 Mar 2021 09:10:12 GMT Content-Type: text/html Content-Length: 39 Connection: keep-alive Last-Modified: Fri, 26 Feb 2021 14:19:32 GMT ETag: "60390374-27" Cache-Control: no-transform Accept-Ranges: bytes Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <html><head></head><body></body></html>
Mar 5, 2021 10:10:12.628387928 CET	153	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: prize-winner-ko3d.live Connection: Keep-Alive Cookie: sid=t4~xrile5icp0uydarybx1kpaml; p1=https://wondertrouble498goal.live/lyxrxqcy/; s1=q8efz1cg6dcbq4e0
Mar 5, 2021 10:10:12.721549034 CET	153	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 05 Mar 2021 09:10:12 GMT Content-Type: image/x-icon Content-Length: 0 Connection: keep-alive Last-Modified: Sat, 06 Jun 2020 22:52:46 GMT Accept-Ranges: bytes ETag: "e2e33b32553cd61:0" Cache-Control: no-transform

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
Mar 5, 2021 10:10:12.995057106 CET	5.189.217.110	443	192.168.2.3	49685	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:12.995471001 CET	5.189.217.110	443	192.168.2.3	49686	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 10:10:13.245964050 CET	5.189.217.110	443	192.168.2.3	49687	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:13.247740030 CET	5.189.217.110	443	192.168.2.3	49688	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:13.254487038 CET	5.189.217.110	443	192.168.2.3	49689	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:13.256184101 CET	5.189.217.110	443	192.168.2.3	49690	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:13.320002079 CET	5.189.217.110	443	192.168.2.3	49691	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 10:10:13.456937075 CET	5.189.217.110	443	192.168.2.3	49695	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:13.463016033 CET	5.189.217.110	443	192.168.2.3	49694	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:13.471767902 CET	5.189.217.110	443	192.168.2.3	49696	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:13.474836111 CET	5.189.217.110	443	192.168.2.3	49697	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:13.555932999 CET	5.189.217.110	443	192.168.2.3	49699	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 10:10:13.559922934 CET	5.189.217.110	443	192.168.2.3	49698	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:13.684708118 CET	5.189.217.110	443	192.168.2.3	49700	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:13.685329914 CET	5.189.217.110	443	192.168.2.3	49701	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:13.709713936 CET	5.189.217.110	443	192.168.2.3	49702	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:13.727058887 CET	5.189.217.110	443	192.168.2.3	49703	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 10:10:13.747986078 CET	5.189.217.110	443	192.168.2.3	49704	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:13.778481007 CET	5.189.217.110	443	192.168.2.3	49705	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:13.787134886 CET	185.50.248.46	443	192.168.2.3	49706	CN=tdsjsext3.life CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Dec 25 13:03:37 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Thu Mar 25 13:03:37 CET 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:13.787926912 CET	185.50.248.46	443	192.168.2.3	49707	CN=tdsjsext3.life CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Dec 25 13:03:37 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Thu Mar 25 13:03:37 CET 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:14.250025988 CET	5.189.217.110	443	192.168.2.3	49709	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 10:10:14.250713110 CET	5.189.217.110	443	192.168.2.3	49708	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:14.339020014 CET	5.189.217.110	443	192.168.2.3	49711	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:14.396207094 CET	5.189.217.110	443	192.168.2.3	49710	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:14.398142099 CET	5.189.217.110	443	192.168.2.3	49712	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:14.470045090 CET	5.189.217.110	443	192.168.2.3	49715	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

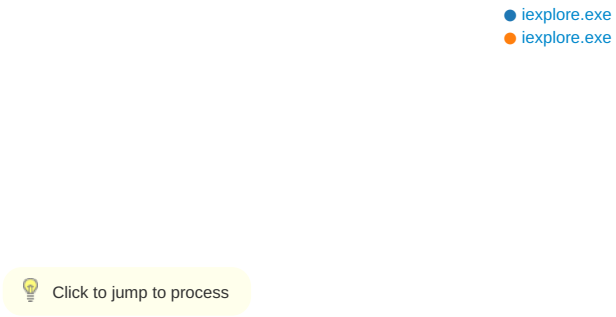
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 10:10:14.472609043 CET	5.189.217.110	443	192.168.2.3	49714	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:14.497338057 CET	5.189.217.110	443	192.168.2.3	49713	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:15.272325993 CET	5.189.217.110	443	192.168.2.3	49716	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:15.353833914 CET	5.189.217.110	443	192.168.2.3	49718	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:15.375503063 CET	5.189.217.110	443	192.168.2.3	49717	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 10:10:28.583734989 CET	5.189.217.110	443	192.168.2.3	49719	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:10:28.586313009 CET	5.189.217.110	443	192.168.2.3	49720	CN=wondertrouble498goal.live CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 04 14:22:33 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 02 15:22:33 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 6112 Parent PID: 792

General

Start time:	10:10:09
Start date:	05/03/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7f7050000
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: 632 Parent PID: 6112

General

Start time:	10:10:10
Start date:	05/03/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6112 CREDAT:17410 /prefetch:2
Imagebase:	0x9f0000
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