ID: 324344
Cookbook: browseurl.jbs
Time: 10:03:04
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

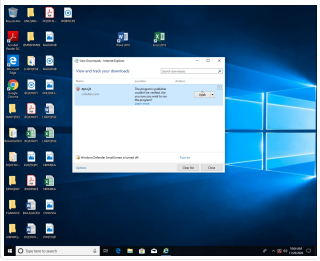
Analysis Report http://cobalten.com/apu.php?zoneid=15…

Overview

General Information

Sample URL:	http://cobalten.com/apu.php?zoneid=1543391
Analysis ID:	324344

Most interesting Screenshot:



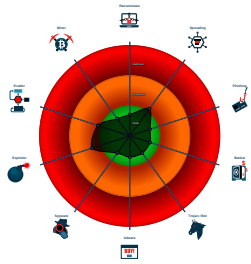
Detection

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

Signatures

- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Found WSH timer for Javascript or V…
- Potential browser exploit detected (p…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6704 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6752 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6704 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - wscript.exe (PID: 6436 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\apu.js' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- **cleanup**

Malware Configuration

No configs have been found

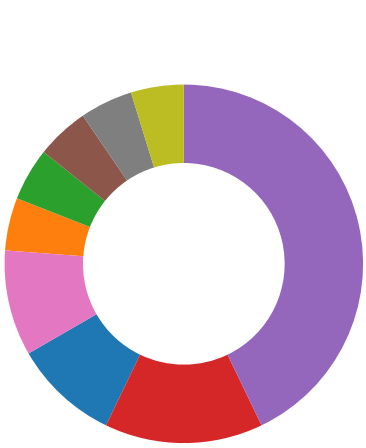
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

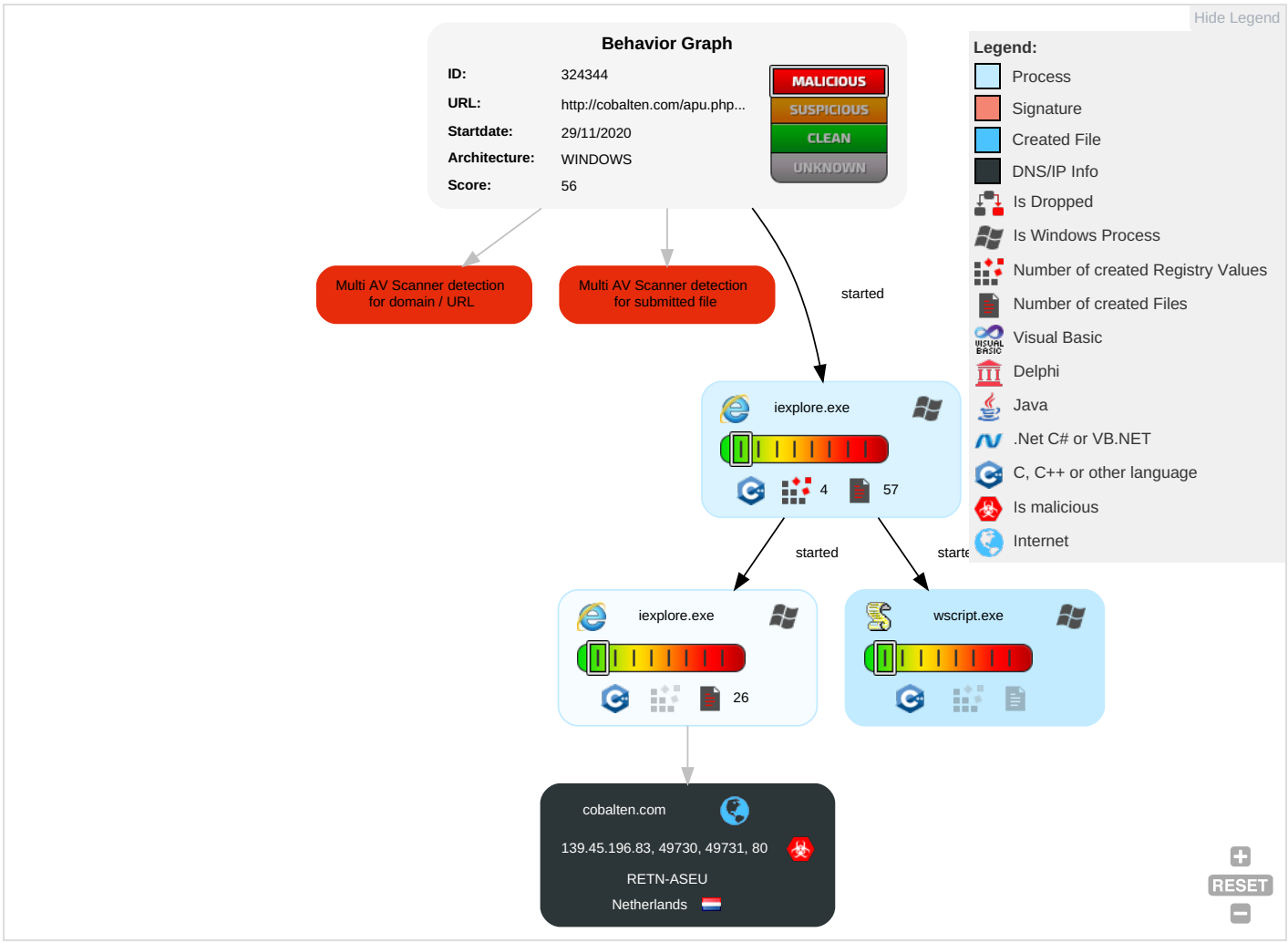
Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

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	Impact
Valid Accounts	Scripting 1	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Process Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Exploitation for Client Execution 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

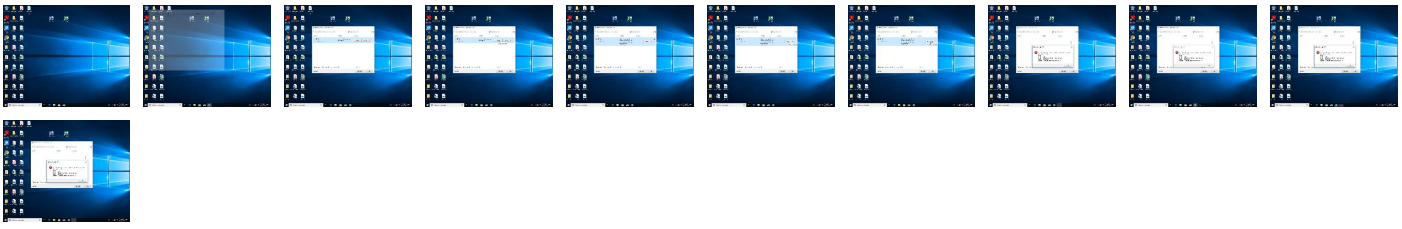
Behavior Graph

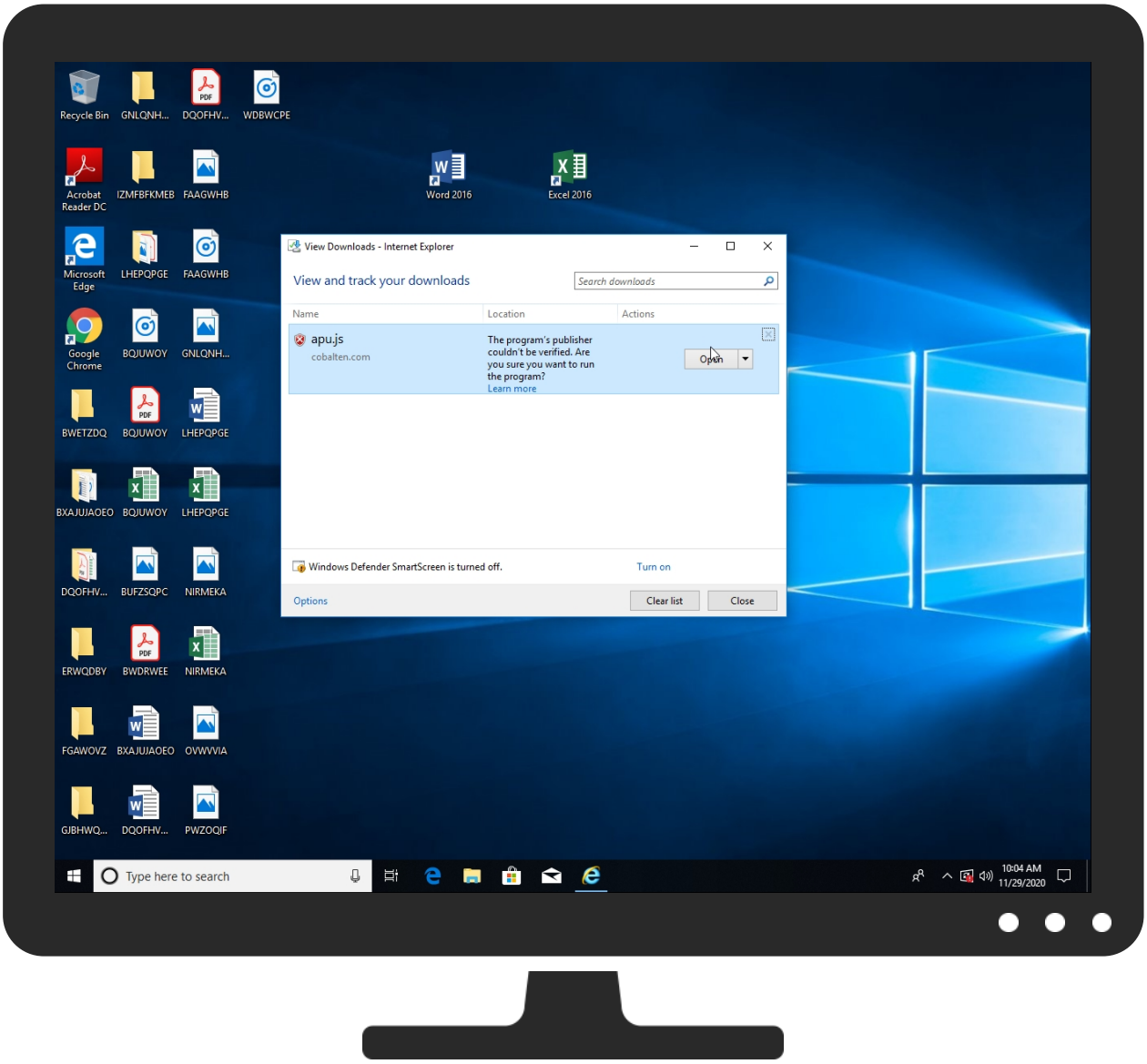


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://cobalten.com/apu.php?zoneid=1543391	6%	Virustotal		Browse
http://cobalten.com/apu.php?zoneid=1543391	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cobalten.com	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://cobalten.com/options?option_args=CN-ZXhlgMmRlNzVmMTY0MmIxNDM5OGJlZjc5ZTZiOTM5OGRkMTIaKmh0dHA6	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
0	1%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cobalten.com	139.45.196.83	true	true	• 6%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://cobalten.com/apu.php?zoneid=1543391	true		unknown
0	true	• 1%, Virustotal, Browse	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://cobalten.com/options?option_args=CN-ZXhlgMmRlNzVmMTY0MmIxNDM5OGJlZjc5ZTZiOTM5OGRkMTIaKmh0dHA6	wscript.exe, 00000007.00000003.701380758.000001BA88B3F000.00000004.00000001.sdmp, wscript.exe, 00000007.00000002.899911273.000001BA88B5F000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
139.45.196.83	unknown	Netherlands		9002	RETN-ASEU	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324344
Start date:	29.11.2020
Start time:	10:03:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://cobalten.com/apu.php?zoneid=1543391
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:	16
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:	mal56.win@5/9@1/1
EGA Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.83.120.32, 93.184.220.29, 51.104.139.180, 152.199.19.161, 13.64.90.137, 40.126.1.135, 40.126.1.144, 20.190.129.18, 40.126.1.143, 40.126.1.129, 20.190.129.23, 20.190.129.1, 20.190.129.134, 52.155.217.156, 104.42.151.234, 20.54.26.129, 67.26.83.254, 67.26.81.254, 8.241.122.254, 8.253.204.249, 8.241.121.126, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, go.microsoft.com, ocsp.digicert.com, login.live.com, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, ie9comview.vo.msecnd.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, login.msa.msidentity.com, ris.api.iris.microsoft.com, go.microsoft.com.edgekey.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtProtectVirtualMemory 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.{C9FB0D29-3221-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	32344
Entropy (8bit):	1.796751689523737
Encrypted:	false
SSDEEP:	192:r9ZaZll299WfztTif2c+zMcWB3QiRkGP1AyXyp2:rTGl89Ufx0fPPF2yt
MD5:	14E3FBB02E4A1E3F4093CBDB2C849CC3
SHA1:	58057F91AA6DD83F30ED46E619123179445FCD88
SHA-256:	110EABAF3E1B741DED95DB1D72F94CE872430D538F6E8E5BC0AE65617DE70D05
SHA-512:	531B42249C72F641A765CCC552CF15E97A2D4C89327FC277DA642BF404DD240C3CBACFE198F68723F555AE64EC8E72001A6D35D53D2A970CB171E1A568CE4D7
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\{C9FB0D2B-3221-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.6006443159742842
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{C9FB0D2B-3221-11EB-90EB-ECF4BBEA1588}.dat	
SSDEEP:	48:Iw/GcprGjGwpa+G4pQOhGrapbSjrGQpBl9WGHHpclOXsTGUpQlCiQGcpm:rVZaQ+6OxBSjFjl9V2lOXk6lgg
MD5:	D46933DC8A8508F0DEF22E85BF63782A
SHA1:	5F1E6ACF5A510E2CC393327DBDE1543E6F374EBE
SHA-256:	CFF602EE4C36BB577A44417725BF19F7CB264CF2E72E3E9146B769C212189D27
SHA-512:	3610CBC47FDC460AE795E1156E24BDDABAFF6E4A4697801C998E3002457786A77594031C2B9056BE146C4D0D4374A073850B168BFE640A84B60294D63DEDCDE
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\apu.js.38x4qq4.partial	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	63244
Entropy (8bit):	5.305075867676128
Encrypted:	false
SSDEEP:	768:zxU7XsA1y2H2wWirIv+XIJYN4b/QQASNOEguYJwjc6n5njZet1mC4HdrGB88q9i7:1UbsA1lrIv+XulNAB9u6Cjy1mjJE8w
MD5:	468803AC7B14D9E67D8533EE74D8E9DA
SHA1:	E0B1B62B16DA21688CFB9E740ABD9AAD5014222F
SHA-256:	C6910AF0DB585874714680D0B8F400A05C0B006733DAAA681B1F58D702411E2D
SHA-512:	28AF18835313C6806F688D3E1B6407D14DA2538902F4651616C13B6DFB3DB5B7F3A0F96CCB971F6F352669111ECA46B74A6A839790D9282CB990EBC44CC7539D
Malicious:	false
Reputation:	low
Preview:	(function(lczxsusin) {function c(e){if(b[e])return b[e].exports;var t=b[e]={exports:{},id:e,loaded:!1};return a[e].call(t.exports,t,t.exports,c),t.loaded=!0,t.exports}var a,b;a=[fu nction(e,t,n){"use strict";var o=r(n(1)),i=n(2),a=r(n(3)),u=n(4),d=r(n(32)),c=r(n(33)),l=n(34),s=n(7),f=n(6),p=n(19),h=r(n(35)),m=n(30),v=n(5),g=n(13),w=r(n(9));n(8);var y=n(29);function r(e){return e&&e.__esModule?e:{default:e}}function b(e){{0,f.addUsedMethod)("initStart");var r="string"==typeof e?JSON.parse((0,l.toString)(e)):e;(0,i.se tOptions)(r);var n=0;if(setInterval(function(){n++,S(r.zoneId,function(e){var t=e.url;(0,i.setOptions)(e),(0,i.setOption)("url",t+(-1<t.indexOf("?")?"&":"?")+"rfo="+n),(0,s.setQual ityParams)(),(0,p.refreshLinks)()})},108e5),(0,m.broadcastInfo)("onclick","0.0.1",r.zoneId,void 0,void 0,{sd:p.setDomain,gum:f.getUsedMethods}),(r.tryToEscapeIframe||r.ge tOutFromIframe)&&a.default.tryTop(),(0,v.isOpenThroughAntiAdblock)()&&setTimeout(function(){(0,h.default)(r.zoneId,"onclick")},100

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\apu.js.38x4qq4.partial:Zone.Identifier	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:gAWY3n:qY3n
MD5:	FBCCF14D504B7B2DBCB5A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443E 8
Malicious:	false
Reputation:	low
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\apu.js:Zone.Identifier	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	very short file (no magic)
Category:	modified
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:W:W
MD5:	ECCBC87E4B5CE2FE28308FD9F2A7BAF3
SHA1:	77DE68DAECD823BABBB58EDB1C8E14D7106E83BB
SHA-256:	4E07408562BEDB8B60CE05C1DECFE3AD16B72230967DE01F640B7E4729B49FCE
SHA-512:	3BAFBF08882A2D10133093A1B8433F50563B93C14ACD05B79028EB1D1279902724145098065199450142 3A66C276AE26C43B739BC65C4E16B10C3AF6C202AEBB
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\apu.js:Zone.Identifier	
Preview:	3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\apu[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	63244
Entropy (8bit):	5.305075867676128
Encrypted:	false
SSDEEP:	768:zxU7XsA1y2H2wWirIv+XIJYN4b/QQASNOEguYJwjc6n5njZet1mC4HdrGB88q9i7:1UbsA1lrIv+XuINAB9u6Cjy1mjJE8w
MD5:	468803AC7B14D9E67D8533EE74D8E9DA
SHA1:	E0B1B62B16DA21688CFB9E740ABD9AAD5014222F
SHA-256:	C6910AF0DB585874714680D0B8F400A05C0B006733DAAA681B1F58D702411E2D
SHA-512:	28AF18835313C6806F688D3E1B6407D14DA2538902F4651616C13B6DFB3DB5B7F3A0F96CCB971F6F352669111ECA46B74A6A839790D9282CB990EBC44CC7539D
Malicious:	false
Reputation:	low
Preview:	(function(lczxsusin) {function c(e){if(b[e])return b[e].exports;var t=b[e]={exports:{},id:e,loaded:!1};return a[e].call(t.exports,t,t.exports,c),t.loaded=!0,t.exports}var a,b;a=[function(e,t,n){"use strict";var o=r(n(1)),i=n(2),a=r(n(3)),u=n(4),d=r(n(32)),c=r(n(33)),l=n(34),s=n(7),f=n(6),p=n(19),h=r(n(35)),m=n(30),v=n(5),g=n(13),w=r(n(9));n(8);var y=n(29);function r(e){return e&&e.__esModule?e:{default:e}}function b(e){(0,f.addUsedMethod)("initStart");var r="string"==typeof e?JSON.parse((0,l.toString)(e)):e;(0,i.setOptions)(r);var n=0;if(setInterval(function(){n++,S(r.zoneId,function(e){var t=e.url;(0,i.setOptions)(e),(0,i.setOption)("url",t+(-1<t.indexOf("?")?"&":"?")+"rfo="+n),(0,s.setQualityParams)(),(0,p.refreshLinks)()})},108e5),(0,m.broadcastInfo)("onclick","0.0.1",r.zoneId,void 0,void 0,{sd:p.setDomain,gum:f.getUsedMethods}),(r.tryToEscapeIframe||r.getOutFromIframe)&&a.default.tryTop(),(0,v.isOpenThroughAntiAdblock)()&&setTimeout(function(){(0,h.default)(r.zoneId,"onclick")},100

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.376382982745554
Encrypted:	false
SSDEEP:	3:oVXVPIMfO75b8JOGXnFPIMfO75+un:o9WMqVqmMq0u
MD5:	28B3CDBBB2DEB560B229EF760BDA5DC3
SHA1:	8A59EBC87777925FE32B755C5A9220376D75AA5D
SHA-256:	52F6CEEE041FD1774C0268E908F9D701BC71DD88D7AA9FA859F971756260D1A5
SHA-512:	E96573353E6711825682A45CED028A0689664E6C170F05EF41242A5A207EC40323EF298A098BC48222259E61C39D0C7E44BB124B542C583192D4530FF7F5B008
Malicious:	false
Reputation:	low
Preview:	[2020/11/29 10:03:48.828] Latest deploy version: ..[2020/11/29 10:03:48.828] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF787EA13DB244596B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	29989
Entropy (8bit):	0.3303862347843544
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwlA9lwlw9l2lm/9l2lz:kBqoxKAuvScS+ljl9lm+ljlCy
MD5:	34D95264272545DD591CDBECA4CF0FB9
SHA1:	8325D66421DA421BECE431BF73E5C96D606E0013
SHA-256:	781B0F673243B0FB06C3BD984B446A8C7D831D24B48249F3E2737B2376D42662
SHA-512:	2000AFC90F607DDF3FFBF412BF880E90CA3F5233081B0A24AC83CCD0BC53FC4090F58405114ED6F823CDA45C30210BC4E676DDCBBA1FF90F8282FF90E95B35 5
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF7D86A71D5668986C.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12981

C:\Users\user\AppData\Local\Temp\~DF7D86A71D5668986C.TMP	
Entropy (8bit):	0.4415542379601371
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRRF9l8fRz9lTq5AoLC:c9lLh9lLh9lIn9lIn9loz9loz9lWs
MD5:	63F15878D07078EFAEE2987386A9FE86
SHA1:	6D49A13E9915A4DCDB4FB0B038AB951C53CAAB8A
SHA-256:	80CEB98819C9FDB3D69747F0ECC0BFCC8AA112E51BECC629966780295F01B739
SHA-512:	30EAE097291797F8274847140C8702DC0EF8498B8308A80894EAAB059292F9C8A23D29DD2FD3BD40193237D6C8EEF6649337416272519C7E407FBAF13C6AD515
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
Nov 29, 2020 10:03:49.936918974 CET	49730	80	192.168.2.4	139.45.196.83
Nov 29, 2020 10:03:49.937750101 CET	49731	80	192.168.2.4	139.45.196.83
Nov 29, 2020 10:03:49.962661982 CET	80	49730	139.45.196.83	192.168.2.4
Nov 29, 2020 10:03:49.962770939 CET	49730	80	192.168.2.4	139.45.196.83
Nov 29, 2020 10:03:49.963325024 CET	80	49731	139.45.196.83	192.168.2.4
Nov 29, 2020 10:03:49.963402987 CET	49731	80	192.168.2.4	139.45.196.83
Nov 29, 2020 10:03:49.964040995 CET	49730	80	192.168.2.4	139.45.196.83
Nov 29, 2020 10:03:49.989686012 CET	80	49730	139.45.196.83	192.168.2.4
Nov 29, 2020 10:03:49.996120930 CET	80	49730	139.45.196.83	192.168.2.4
Nov 29, 2020 10:03:49.996169090 CET	80	49730	139.45.196.83	192.168.2.4
Nov 29, 2020 10:03:49.996191978 CET	49730	80	192.168.2.4	139.45.196.83
Nov 29, 2020 10:03:49.996202946 CET	80	49730	139.45.196.83	192.168.2.4
Nov 29, 2020 10:03:49.996220112 CET	49730	80	192.168.2.4	139.45.196.83
Nov 29, 2020 10:03:49.996246099 CET	80	49730	139.45.196.83	192.168.2.4
Nov 29, 2020 10:03:49.996263027 CET	49730	80	192.168.2.4	139.45.196.83
Nov 29, 2020 10:03:49.996294022 CET	80	49730	139.45.196.83	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 10:03:49.996304035 CET	49730	80	192.168.2.4	139.45.196.83
Nov 29, 2020 10:03:49.996335030 CET	80	49730	139.45.196.83	192.168.2.4
Nov 29, 2020 10:03:49.996349096 CET	49730	80	192.168.2.4	139.45.196.83
Nov 29, 2020 10:03:49.996377945 CET	80	49730	139.45.196.83	192.168.2.4
Nov 29, 2020 10:03:49.996387959 CET	49730	80	192.168.2.4	139.45.196.83
Nov 29, 2020 10:03:49.996413946 CET	80	49730	139.45.196.83	192.168.2.4
Nov 29, 2020 10:03:49.996438026 CET	49730	80	192.168.2.4	139.45.196.83
Nov 29, 2020 10:03:49.996459961 CET	80	49730	139.45.196.83	192.168.2.4
Nov 29, 2020 10:03:49.996478081 CET	49730	80	192.168.2.4	139.45.196.83
Nov 29, 2020 10:03:49.996500969 CET	80	49730	139.45.196.83	192.168.2.4
Nov 29, 2020 10:03:49.996537924 CET	49730	80	192.168.2.4	139.45.196.83
Nov 29, 2020 10:03:49.996550083 CET	49730	80	192.168.2.4	139.45.196.83
Nov 29, 2020 10:03:50.022214890 CET	80	49730	139.45.196.83	192.168.2.4
Nov 29, 2020 10:03:50.022252083 CET	80	49730	139.45.196.83	192.168.2.4
Nov 29, 2020 10:03:50.022283077 CET	49730	80	192.168.2.4	139.45.196.83
Nov 29, 2020 10:03:50.022298098 CET	80	49730	139.45.196.83	192.168.2.4
Nov 29, 2020 10:03:50.022325039 CET	49730	80	192.168.2.4	139.45.196.83
Nov 29, 2020 10:03:50.022330999 CET	80	49730	139.45.196.83	192.168.2.4
Nov 29, 2020 10:03:50.022346973 CET	49730	80	192.168.2.4	139.45.196.83
Nov 29, 2020 10:03:50.022360086 CET	80	49730	139.45.196.83	192.168.2.4
Nov 29, 2020 10:03:50.022392035 CET	49730	80	192.168.2.4	139.45.196.83
Nov 29, 2020 10:03:50.022399902 CET	80	49730	139.45.196.83	192.168.2.4
Nov 29, 2020 10:03:50.022403955 CET	49730	80	192.168.2.4	139.45.196.83
Nov 29, 2020 10:03:50.022433996 CET	80	49730	139.45.196.83	192.168.2.4
Nov 29, 2020 10:03:50.022454023 CET	49730	80	192.168.2.4	139.45.196.83
Nov 29, 2020 10:03:50.022481918 CET	49730	80	192.168.2.4	139.45.196.83
Nov 29, 2020 10:03:54.996385098 CET	80	49730	139.45.196.83	192.168.2.4
Nov 29, 2020 10:03:54.996725082 CET	49730	80	192.168.2.4	139.45.196.83
Nov 29, 2020 10:04:02.194062948 CET	49730	80	192.168.2.4	139.45.196.83
Nov 29, 2020 10:04:02.219938040 CET	80	49730	139.45.196.83	192.168.2.4
Nov 29, 2020 10:04:02.227606058 CET	49731	80	192.168.2.4	139.45.196.83

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 10:03:48.832676888 CET	53097	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:03:48.869710922 CET	53	53097	8.8.8.8	192.168.2.4
Nov 29, 2020 10:03:49.890487909 CET	49257	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:03:49.925926924 CET	53	49257	8.8.8.8	192.168.2.4
Nov 29, 2020 10:03:56.968848944 CET	62389	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:03:56.996298075 CET	53	62389	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:17.220031023 CET	49910	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:17.247478962 CET	53	49910	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:18.823914051 CET	55854	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:18.863179922 CET	53	55854	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:19.255518913 CET	64549	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:19.291258097 CET	53	64549	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:19.827651978 CET	55854	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:19.863396883 CET	53	55854	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:20.830734015 CET	55854	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:20.866213083 CET	53	55854	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:22.453840017 CET	63153	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:22.490827084 CET	53	63153	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:22.562586069 CET	52991	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:22.599355936 CET	53	52991	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:22.846357107 CET	55854	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:22.881577969 CET	53	55854	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:23.023591042 CET	53700	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:23.079916000 CET	53	53700	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:23.466439009 CET	51726	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:23.501782894 CET	53	51726	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:23.647947073 CET	56794	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:23.674860954 CET	53	56794	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:24.192768097 CET	56534	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 10:04:24.230690002 CET	53	56534	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:24.807898998 CET	56627	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:24.843483925 CET	53	56627	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:24.879498005 CET	56621	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:24.891875982 CET	63116	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:24.918977976 CET	53	63116	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:24.923193932 CET	53	56621	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:25.212330103 CET	64078	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:25.248246908 CET	53	64078	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:25.653007030 CET	64801	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:25.688878059 CET	53	64801	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:26.185631990 CET	61721	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:26.221194983 CET	53	61721	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:26.302387953 CET	51255	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:26.329488993 CET	53	51255	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:26.830339909 CET	61522	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:26.862430096 CET	55854	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:26.865880966 CET	53	61522	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:26.900038958 CET	53	55854	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:27.251632929 CET	52337	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:27.278814077 CET	53	52337	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:27.369324923 CET	55046	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:27.404973030 CET	53	55046	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:28.603399992 CET	49612	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:28.639071941 CET	53	49612	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:29.618382931 CET	49285	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:29.645915985 CET	53	49285	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:30.717787027 CET	50601	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:30.745055914 CET	53	50601	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:31.743808985 CET	60875	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:31.771111012 CET	53	60875	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:32.807871103 CET	56448	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:32.835032940 CET	53	56448	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:33.316510916 CET	59172	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:33.343626976 CET	53	59172	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:34.089165926 CET	62420	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:34.116295099 CET	53	62420	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:35.219573021 CET	60579	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:35.246833086 CET	53	60579	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:36.208369970 CET	50183	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:36.244106054 CET	53	50183	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:37.914171934 CET	61531	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:37.941526890 CET	53	61531	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:39.007266045 CET	49228	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:39.043148994 CET	53	49228	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:40.089257956 CET	59794	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:40.116472960 CET	53	59794	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:41.432390928 CET	55916	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:41.459590912 CET	53	55916	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:42.604558945 CET	52752	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:42.631647110 CET	53	52752	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:43.709355116 CET	60542	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:43.736694098 CET	53	60542	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:44.821275949 CET	60689	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:44.848459005 CET	53	60689	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:51.890614033 CET	64206	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:51.901263952 CET	50904	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:51.917781115 CET	53	64206	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:51.936786890 CET	53	50904	8.8.8.8	192.168.2.4
Nov 29, 2020 10:04:55.120908022 CET	57525	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:04:55.156374931 CET	53	57525	8.8.8.8	192.168.2.4
Nov 29, 2020 10:05:26.084811926 CET	53814	53	192.168.2.4	8.8.8.8
Nov 29, 2020 10:05:26.112126112 CET	53	53814	8.8.8.8	192.168.2.4
Nov 29, 2020 10:05:27.608913898 CET	53418	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 10:05:27.660434008 CET	53	53418	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 29, 2020 10:03:49.890487909 CET	192.168.2.4	8.8.8.8	0xa10	Standard query (0)	cobalten.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 29, 2020 10:03:49.925926924 CET	8.8.8.8	192.168.2.4	0xa10	No error (0)	cobalten.com		139.45.196.83	A (IP address)	IN (0x0001)
Nov 29, 2020 10:03:49.925926924 CET	8.8.8.8	192.168.2.4	0xa10	No error (0)	cobalten.com		139.45.196.21	A (IP address)	IN (0x0001)
Nov 29, 2020 10:03:49.925926924 CET	8.8.8.8	192.168.2.4	0xa10	No error (0)	cobalten.com		139.45.195.158	A (IP address)	IN (0x0001)
Nov 29, 2020 10:03:49.925926924 CET	8.8.8.8	192.168.2.4	0xa10	No error (0)	cobalten.com		139.45.195.37	A (IP address)	IN (0x0001)
Nov 29, 2020 10:03:49.925926924 CET	8.8.8.8	192.168.2.4	0xa10	No error (0)	cobalten.com		139.45.197.8	A (IP address)	IN (0x0001)
Nov 29, 2020 10:03:49.925926924 CET	8.8.8.8	192.168.2.4	0xa10	No error (0)	cobalten.com		139.45.195.102	A (IP address)	IN (0x0001)
Nov 29, 2020 10:04:22.490827084 CET	8.8.8.8	192.168.2.4	0x97c8	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- cobalten.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49730	139.45.196.83	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 29, 2020 10:03:49.964040995 CET	2	OUT	GET /apu.php?zoneid=1543391 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: cobalten.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Nov 29, 2020 10:03:49.996120930 CET	3	IN	HTTP/1.1 200 OK Server: nginx Date: Sun, 29 Nov 2020 09:03:49 GMT Content-Type: application/javascript Transfer-Encoding: chunked Connection: keep-alive Access-Control-Allow-Origin: * Access-Control-Allow-Credentials: true Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Allow-Headers: Accept, Content-Type, Content-Length, Accept-Encoding Pragma: no-cache Cache-Control: no-transform, no-store, no-cache, must-revalidate, max-age=0 Expires: Tue, 11 Jan 1994 10:00:00 GMT Timing-Allow-Origin: * X-Trace-Id: f83dd63a37d5c263aa2364f4c65ffdf5 Set-Cookie: OAID=2de75f1642b14398bef79e6b9398dd12; expires=Mon, 29 Nov 2021 09:03:49 GMT Set-Cookie: oaidts=1606640629; expires=Mon, 29 Nov 2021 09:03:49 GMT Strict-Transport-Security: max-age=1 X-Content-Type-Options: nosniff Timing-Allow-Origin: * Content-Encoding: gzip Data Raw: 35 35 30 33 0d 0a 1f 8b 08 00 00 00 00 00 04 03 cd bd 0b 5f db 56 d6 f0 fb 55 40 f3 be 8c 1d 8c b9 24 69 1b 1c 97 93 90 a4 a1 4d 02 0d 64 7a a1 4c 7e c2 16 a0 62 4b 1e 59 86 10 e0 7c f6 f3 5f 6b ef 2d 6d d9 32 a1 9d ce 9c 79 9e 69 b0 a4 7d df 6b af fb 5a bb 71 32 49 7a 79 9c 26 8d 41 ef f3 a7 f1 64 1c 27 cd 85 6b f7 72 a1 d7 88 9a d7 f1 49 e3 f8 30 3a 6a 66 51 3e c9 92 05 f9 dd 8e 3e 8d d2 2c 1f 77 2e c2 6c 21 ef ca ab ee b5 7d b7 79 7d db 8a fb 9b 51 6b 90 86 fd a8 bf b9 b8 7e db b1 55 43 a9 da 0b 07 83 46 ee 5a 68 e5 ad f2 77 af c9 83 a9 d6 5d 5c 2b 3f dc 4a 37 61 eb b8 13 76 0f dd d8 1a 11 55 93 e6 75 30 19 47 0b e3 3c 8b 7b 79 a0 c3 49 bb 59 23 69 ac 37 9b ad b8 9b 34 36 9a ad 50 5f 3c e4 c5 84 17 8f 9a ad be 79 b1 c1 9b 9e f9 29 1f 07 7c 7c c8 d7 31 7f bf 6e b6 4e f8 f3 55 b3 35 e2 cf fa 93 66 eb cc 14 7c 4c c1 a1 14 5c 6b b6 2e f8 fb b8 d9 3a 95 12 0f 9b ad 4b 2d f1 a4 d9 ec 24 8d 6f 9a 3a 94 2b 3e 6d 3c 69 76 dc 98 17 32 59 4f bb 18 d1 d2 52 d4 fe f8 31 1a bf 4d fb 93 41 b4 15 6d 5e f7 a3 93 70 32 c8 37 a3 db db a2 ca b1 54 69 ac b5 4e da 61 bf ff 61 1c f5 df 46 f9 59 da 6f 36 82 38 89 f3 fd 3c cc f2 c0 f4 96 75 03 59 87 e4 34 e8 76 f3 ab 51 94 9e 2c 44 5b df ef ef be 6b 8f c2 6c 1c 35 68 64 d0 ce d3 7d 2d d3 a4 d9 e6 66 d4 e1 65 dc 1e 47 f9 ee 48 a0 60 dc 6c 64 a6 b1 a4 bb d6 61 e3 f9 b2 93 e4 51 76 11 0e 1a 6e 48 8d e6 75 b2 bc dc da 6f 64 ed cf 69 12 ed f4 5b c5 17 86 6a 20 22 6a 4f b2 c1 6c e3 51 b3 55 ed 90 69 50 30 68 e5 Data Ascii: 5503_VU@$iMdzL~bKY|_k-m2yi}kZq2Izy&Ad'krl0:jfQ>>,w.l!}y}Qk~UCFZhw]\+?J7avUu0G<{ylY#i746P _<y)\|1nNU5f\|L\k.:K-$o:+>m<iv2YOR1MAm^p27TiNaaFYo68<uY4vQ,D[kl5hd}-feGH`ldaQvnHuodi[j "jOlQUiP0h

Code Manipulations

Statistics

Behavior

- iexplore.exe
- iexplore.exe
- wscript.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6704 Parent PID: 800

General

Start time:	10:03:47
Start date:	29/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff60e6e0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 6752 Parent PID: 6704

General

Start time:	10:03:48
Start date:	29/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6704 CREDAT:17410 /prefetch:2
Imagebase:	0xed0000
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

Analysis Process: wscript.exe PID: 6436 Parent PID: 6704

General

Start time:	10:04:16
Start date:	29/11/2020
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\apu.js'
Imagebase:	0x7ff773b00000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis