ID: 438533
Cookbook: browseurl.jbs
Time: 18:09:49
Date: 22/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

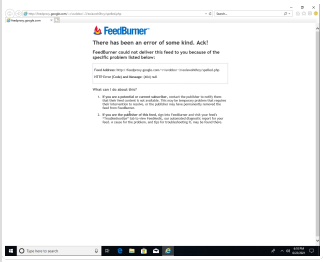
Windows Analysis Report http://feedproxy.google.com/...

Overview

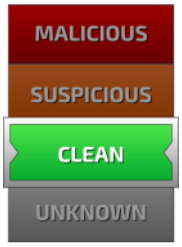
General Information

Sample URL:	http://feedproxy.google.com/~r/uvdobo/~3/eoiawoh0hcy/spelled.php
Analysis ID:	438533
Infos:	

Most interesting Screenshot:



Detection

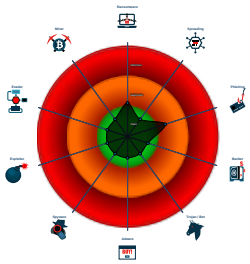


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found iframes
- Unusual large HTML page

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 5424 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4552 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5424 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

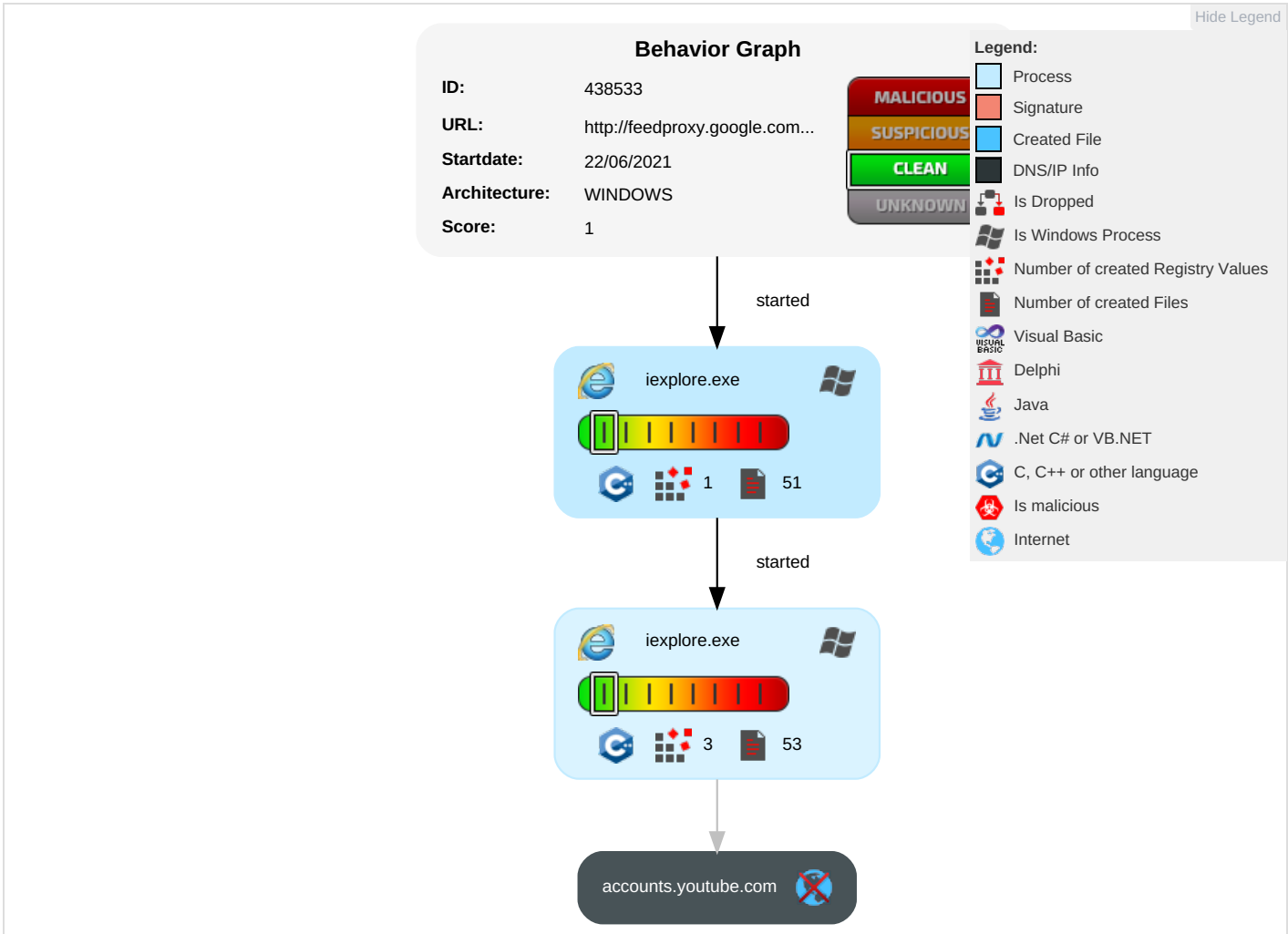
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

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	Im
Drive-by Compromise 1	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	Non-Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mo Sy Pa
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	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De Lo

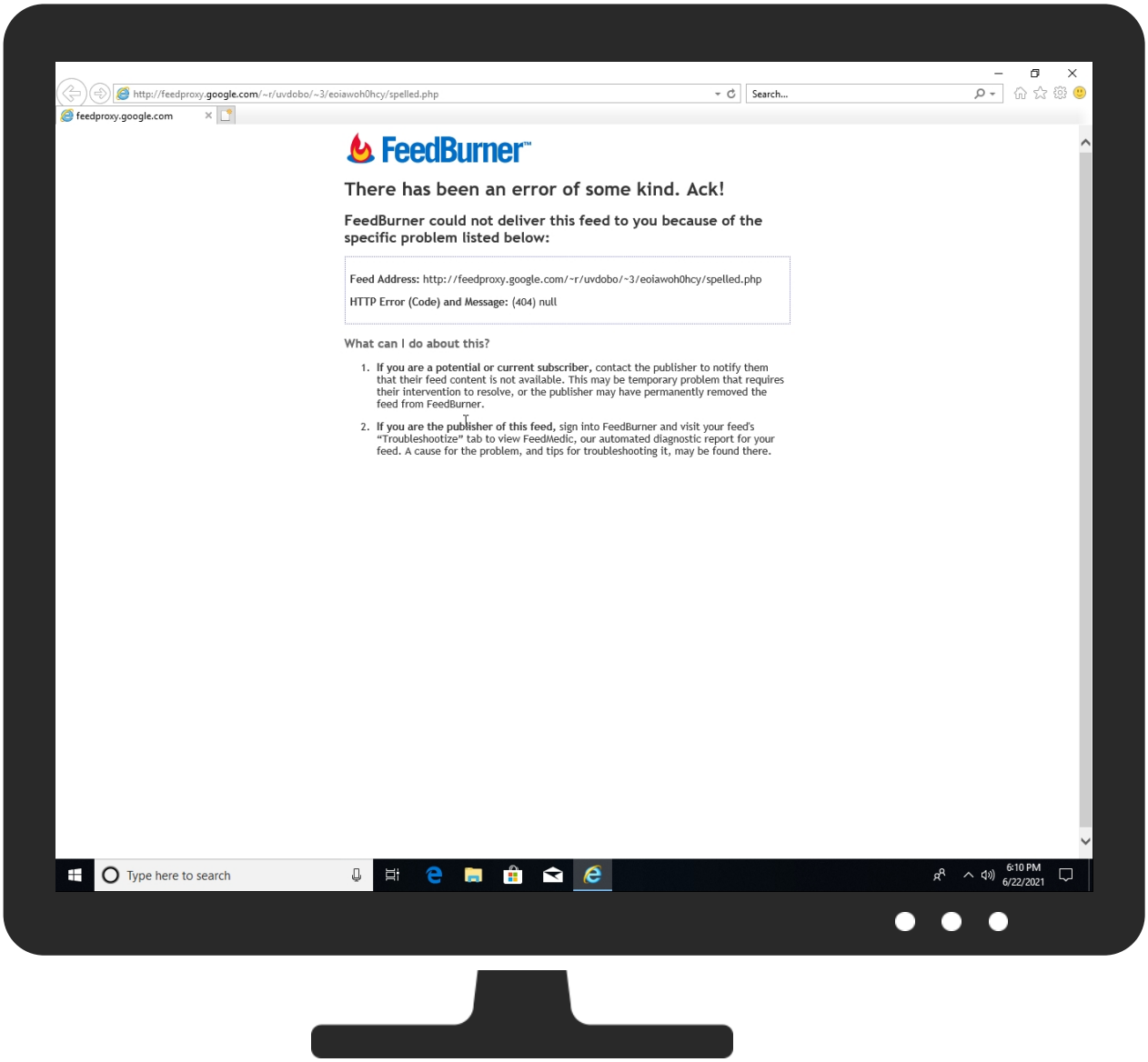
Behavior Graph



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://feedproxy.google.com/~r/uvdobo/~3/eoiawoh0hcy/spelled.php	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://accounts.googl	0%	URL Reputation	safe	
http://https://accounts.googl	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://accounts.googl	0%	URL Reputation	safe	
http://https://accounts.googl	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.youtube.com	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	438533
Start date:	22.06.2021
Start time:	18:09:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://feedproxy.google.com/~r/uvdobo/~3/eoiawoh0hcy/spelled.php
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:	6
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:	CLEAN
Classification:	clean1.win@3/26@1/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://feedburner.google.com/
Warnings:	Show All

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\DOMStore\E5F0NRSV\accounts.google[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	106
Entropy (8bit):	4.4342841931232515
Encrypted:	false
SSDEEP:	3:D90aK1r0aK1ryRtFwsoIcDAqFf3PqI9qSeWcbwbFKb:JFK1rFK1rUFxmAq93dlebbwwb
MD5:	4920B6944D5119D8065CC9C41599A9BD
SHA1:	A2A472AE5B8407EC706AD1295B23103F9D27BCC4
SHA-256:	6B00DE1CA0B26F55D3C22E869E9AB9B0D1C76572F89BE07B4C6C9EFE8E1531EF
SHA-512:	67F1CE5C2CBBCD8635D49196ECA2ABAF979092226D1A655DFA71EBF72DD9038D7C44B5269AEDAE94B8B50680174DB450F3B5B47A21927D804866D9776724DB 6
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root><item name="promo" value="{}" ltime="792458912" htime="30893953" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{5EB6A9E6-D374-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.851613691647451
Encrypted:	false
SSDEEP:	192:r/ZgZe2TWutrift5wqzMdiBf98DBsffwzjX:rhwVqOMtc4fkk4
MD5:	36A70AD46592701B360289883938F202
SHA1:	A1F34BB740114397ACF11FCA9F58DA90B421102E
SHA-256:	3F1C7E7F1D508C7A9277143FD4ACF433F12348043ACB2974FADCAFC432D11D4E
SHA-512:	910480E1B7A5CB111BC68BD3C3D46537C9BD29145627878B64138435BC688AA1701E5E7D7DB2C757349B8E44DEF930EF032668CEBABBDE30CFF910489F66022
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\{5EB6A9E8-D374-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	42256
Entropy (8bit):	2.1528124869196823
Encrypted:	false
SSDEEP:	192:r5ZeQK6Dkwjx2uWDMrLVpTFs8m/R1kCg50DpT6sk0o6sbR1RsCUo6sbR1RsWILs0:rvb1IyglAnrTNa7VT/oJ0oJMpxz
MD5:	8DA5BE88986569E769811845832D2379
SHA1:	9D9D48117E97E5AFBDF96FDB83A248C1F10119A6
SHA-256:	725CB6233BDB143572E07624269BC4B35B2D73B07605800CFA2D8131D508D912
SHA-512:	B5D3BFD2DA43D6D45E39CF265D8DDD4FD35828C707A845C1084B6652BD54A2BE20DA3F8E3935E6B3A553CD0919E7208F1C5B3A482F296C94AD535AD8C093AE8
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\{5EB6A9E9-D374-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.564593769782458
Encrypted:	false
SSDEEP:	48:IwJGcprUGwpaBG4pQhGrapbS4GQpKSG7HpRxTGIpG:rPZsQT6xBSAA9TnA
MD5:	2CA979218B73C9026585ADBE9D0AB877
SHA1:	04CB319DB55D24D32415CB3091D82C6DFC0C8493
SHA-256:	FDA0FE6D445373B7C36B3CFB53FE79E29A236AFB1A99CDDC6774A2EB5621D0F4
SHA-512:	91D26F925DC17A13589F8617DBCADAC13BC26C7188D156605C219B43323816419216B0F4E07EC2AA9DFAA45131FA8CADD4A16664495F9845DD83E87AC492164
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	5648
Entropy (8bit):	3.741590616748009
Encrypted:	false
SSDEEP:	48:xwDaO7IJct3xI5wDaYxG/7nvWDtZcdYLtX7B6QXL3aqG8X:YvIJct+QP47v+rcqlBPG9C
MD5:	16602D270E5232389B67C6CF040E05D8
SHA1:	EBAF5133848159BC57F844D05148BFC5E9DED133
SHA-256:	5524F7EF371A703839F21B6F564BFF06BF3C9B6511645A23CE1101B69287EEEB
SHA-512:	B9151DE3A5E386BF7F06556413C29D80339168ECF87FA125C51D8A39233654D6F254D205A79F8890080AEC4B5174DFC6306AAD04591FBECAB9A95B9220264E02
Malicious:	false
Reputation:	low
Preview:	".h.t.t.p.s.:./.w.w.w...g.o.o.g.l.e...c.o.m./.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... ....0..... .....v.].X..:.X.:.r.Y.....q.X.S.4.S.4.S.4.S.4.S.4.S.4...X.....0.....q.W.S.4.X.:.....J...A...g.....K.H.V. 8.....F..B.....B.....B..B..B..B..B...u.....B..B..B..B..B...{.....5.....k..... .....7R..8F.....2.....Vb..5C..;I.....R^.....0.....Xc..5C..5C..5C..5C..5C..5C..lv..... .....]i..<J..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\KFOlCnqEu92Fr1MmEU9fBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20012, version 1.1
Category:	downloaded
Size (bytes):	20012
Entropy (8bit):	7.966842359681559
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\KFOlCnqEu92Fr1MmEU9fBBc-[1].woff	
SSDEEP:	384:Yc6bX9TagDCXKqs4+W5XVgaflKHjsGdZtlh3K/qzWz/scZpuB:YcCVaeCaF4ea9KHYQZtlh3Kgy4B
MD5:	DE8B7431B74642E830AF4D4F4B513EC9
SHA1:	F549F1FE8A0B86EF3FBDCB8D508440AFF84C385C
SHA-256:	3BFE46BB1CA35B205306C5EC664E99E4A816F48A417B6B42E77A1F43F0BC4E7A
SHA-512:	57D3D4DE3816307ED954B796C13BFA34AF22A46A2FEA310DF90E966301350AE8ADAC62BCD2ABF7D7768E6BDCBB3DFC5069378A728436173D07ABFA483C1025AC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc-.woff
Preview:	wOFF.....N,.....GDEF.....G...d....GPOS.....GSUB.....7b..OS/2.....R...`t.#.cmap...4.....L....cvt .....\...\1..Kfpgm...@...2.....$.gasp...t.....glyf.....:..j.'..hdmx..G,...f.....head..G....6...6...rhhea..G.....$....hmtx..G....a.....MOloca..JP.....\v@zmaxp..L,... ... .name..LL.....:.post..M(..... .m.dprep..M<.....S...)x...1..P.....PB..U.=I.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R.....2.x...pfK.G...1.c>..`9..m<+;..m.x...bg.M.T...O.....l...XU.../{.[_..W....c._..72.. ." z.+..F.....&.&...`e..T].....K=..K2S....q..d...xf.$~i..$?.d..dU.....@R-/LMO-J6...[]..Z..O.C_."lf..d....fS....$d.G>eL`....Tf1.....9.c>..`1.TR..x./d-.....q.....7....{...v.....!.....1.QG=.4.D3-..F;=..1'.'q.rw...9..e!.....Q....f.....qV.n.h.V.Z]..B..C.[B...V.....v...o.w.{...w..zRO.i=..._.....-.m....].=...[...(1.(.#.....O0/.0?..04rL.G.9.....i6..l..|.(o.....\|$,..{|&|....YJ...x.e8B.#..t;R8.{+....\=.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\KFOmCnqEu92Fr1Mu4mxM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19824, version 1.1
Category:	downloaded
Size (bytes):	19824
Entropy (8bit):	7.970306766642997
Encrypted:	false
SSDEEP:	384:ozNCb8EbW9Wg166uwroOp/taiap3K6MC4fsPPuzt+7NCXzS65XZELt:K4zbWcDVwt230hfs+x+Bb65X2
MD5:	BAFB105BAEB22D965C70FE52BA6B49D9
SHA1:	934014CC9BBE5883542BE756B3146C05844B254F
SHA-256:	1570F866BF6EAE82041E407280894A86AD2B8B275E01908AE156914DC693A4ED
SHA-512:	85A91773B0283E3B2400C773527542228478CC1B9E8AD8EA62435D705E98702A40BEDF26CB5B0900DD8FECC79F802B8C1839184E787D9416886DBC73DFF22A64
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxM.woff
Preview:	wOFF.....Mp.....P.....GDEF.....G...d....GPOS.....hGSUB.....7b..OS/2.....R...`tq#.cmap.....L....cvt .....T...T+...fpgm.....5....w.`.gasp...@.....glyf...L..:+..j.....hdmx..Fx...g.....head..F....6...6.j.zhhea..G.....$....hmtx..G8...]......Vlloca..I.....?.#.maxp..Kt... ... .name..K.....t.U9.post..Ld..... .m.dprep..Lx.....I.f..x...1..P.....PB..U.=I.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R.....2.x.....[....#N..m.m.m.mfm....SP..NuM..9]..=.U..!...[.....w...|.....^p....H.....;...).....;..EoDo....E.E.D..`.0.GG.aA.H.V.Mx\xA...../..d3.Eb_.J...R.^v.....\^ob.}.z..k.x).v$f$..O)+.2..*....y}6`C6b.6cs...I.....!.....<..|..|..|..|..|....o....I%.4.L.SI.&C.6..!`...{...c..\.J.(.2.C....V.A..?.M<nG.....v..m.;..R.C..aj.H...=..{.>.:.....}i_Y.....:....o.&k..KY.2..6k....i]..{..p}../.....VO3.o].fJ....R-TZ..;...RN..&V...C...3.?.....&..z.s&.D....r,.I...t.R..a$k..Mm..Y.U...+b.%kQ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\m=i5H9N,sy6v,sy70,PHUlyb,qNG0Fc,ywOR5c[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	modified
Size (bytes):	37948
Entropy (8bit):	5.646981597659815
Encrypted:	false
SSDEEP:	768:LFpt9yZNxKKS4j2rI+Xz9YzLHNw1Mg39c2w2Xj3XAZ0XUqwFWK:BDcMkj2rIg9u+EysZtN
MD5:	04CD2CFD1C7DD6447768A9AB86D3FEE2
SHA1:	E5713D67B24402B5D5F8E38A0240C2EFCE980D88
SHA-256:	222AAE30C474BFBED2943CAAED885A8F205625830FE2723C276240AC2322720A
SHA-512:	5BA9DEDA2691F7CD078A151A346648BF3ADFA9C217438934E8303D2E977842F0D3453B984E537F125D69DB9E56E4984036343807F4D714E0005D254F1A168D47
Malicious:	false
Reputation:	low
Preview:	this._G=this._G||{};(function(_){var window=this;.try{._.k("i5H9N");._.aS=function(a){_.Fv.call(this,a.Da);this.ka=this.Tb=this.aa=this.Ga=this.ha=this.ra=null;this.focused=!1;this.Oa=30;this.Oc="INACTIVE";this.zb=new _.Il(0,0);this.ea=_.sC(_.tC(this).Sc(this.Kf).Je());_.YI.has(this.Af());this.Ca().Qb("aria-multiselectable")};_.x(_.aS,_.Fv);_.aS.ta=_.Fv.ta;var bS=function(a){return"true"!==a.Qb("aria-disabled")};_.h=_.aS.prototype;_.h.Cb=function(a,b){b?a.Bd("aria-disabled"):a.qb("aria-disabled",!0);return this};_.h.Vx=function(){return this.aa};_.h.MI=function(){return this.Tb};_.h.px=function(){this.aa=null;this.ea()};_.h.Vb=function(){return this.focused};_.h.QJ=function(a){var b=a.da;bS(b)&&(b=_.jg.has(_.ZI(b))?b:a.aa,!bS(b)||"INACTIVE"!==this.Oc||1!==a.event.which&&"number"===typeof a.event.which||(this.ka=a,this.Oc="HOLDING",cS(this,a.event),this.Ed(b)))};_.h.Sv=function(a){this.focused&&(this.focused=!1);cS(this,a.event);if("HOLDING"===this.Oc||"ACTIVE_HOLDING"===this.Oc)this.a

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\m=sy6w,i5dxUd,m9oV,RAnnUd,sy6q,sy6r,sy6s,uu7UOe,sy6t,sy6u,soHxf[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	25548
Entropy (8bit):	5.592456714853886
Encrypted:	false
SSDEEP:	768:KdY94iMm+2rP65VK2pvm/V9SPPphsWfct:KdYCiS2ryP5Jn2
MD5:	061948C2DFEEDC2E4AFC91EA5BB422B8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\m=sy6w,i5dxUd,m9oV,RAnnUd,sy6q,sy6r,sy6s,uu7UOe,sy6t,sy6u,soHxf[1].js	
SHA1:	555610CD88A072DD628B16B041037C96FE6126CC
SHA-256:	A5772554DAEFF688BA22F9E93121C23BB7C1529FE10ACAC42CA9556799C21DBA
SHA-512:	8F05FF4A50FFC689404A1D0227B0532417C686E356F4BE3DEB6F560CC7642C8C8955BEE3D75F5F86593B4C298FFBFFC1B0888F079F20EC18E3A161B73F7491A7
Malicious:	false
Reputation:	low
Preview:	this._G=this._G||{};(function(_){var window=this;.try{._.k("sy6w");./*.. Copyright 2016 Google Inc... Permission is hereby granted, free of charge, to any person obtaining a copy. of this software and associated documentation files (the "Software"), to deal. in the Software without restriction, including without limitation the rights. to use, copy, modify, merge, publish, distribute, sublicense, and/or sell. copies of the Software, and to permit persons to whom the Software is. furnished to do so, subject to the fo llowing conditions:.. The above copyright notice and this permission notice shall be included in. all copies or substantial portions of the Software... THE SOFTWARE IS PR OVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR. IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,. FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE. AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAI M, DAMAGES OR OTHER. LIABILITY, WHETHER IN AN ACTI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\v2logo_white[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 230 x 42
Category:	downloaded
Size (bytes):	2179
Entropy (8bit):	7.611313616692605
Encrypted:	false
SSDEEP:	48:AbFb/8jdiP5vL+wOf/+aNzRU6fGxwBAtP5onBsUQ:AwmZLvidZu6c1yBVQ
MD5:	FE2D4E977BC38C16CE8302142AA8C53E
SHA1:	E2579946A0222E4F811514C008A340F103145748
SHA-256:	DDC2AEDFCFEBDAC60B011AA814289CFB8DB2FD23449531BF9B2EE9273CC0CB42
SHA-512:	246BBE5681F8FD3EADD1D7BF749AD5D62166B66459D1154A59F2E66CF013D56DCB115607254FC0F80BCBDD3508C89DB0270A44861FA3EACAC83E5305D312466
Malicious:	false
Reputation:	low
IE Cache URL:	http://feedburner.google.com/fb/images/v2logo_white.gif
Preview:	GIF89a..*.....n.....8...9V.....H'z...b..8q.v....U.....P....Jb.....-.{..K.h.6..... .....VJ...../...+H....Yp....0*....k''...k.....u.._$.;U..;*\....t.....h}....2h_.....<(.....A.S%"...$+.....~..@... ...x.....v!.....5..*.....s.....!.....,.....*.....?.....)*.....%.....-) .....*.)..B....B.(.?....A...%.) .....B.?...D6#..?..).....0o.*{ .x.h..:v...(...._."...P#9..w...Ba.r..)s..''..0..hG0$.....d...l.....sAljZ.s.....X.A.Z..YN..M..a2..X.d..`..l<AB....H.C.g.6$M. .X...-..l.t...x...?C....*.`.l?.-.... ..m.L.s.B(.....!.%.....r{9.$,h.@....!.....x0a.H.d.?F..9Q...x...^.xB3...X..nq6h+..[...r...+.4.....G...t(...''...V.l.lw..@.>D.faD...\.=6...0!.m..w.8..S. ...8M.....2./.x.B!!.s.#..B''.C...Q.?<`NJ.... ..CDh.=..9...b;<...^K..%n1..H1....1..b.=% YN.M..C..|PS.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\KFOkCnqEu92Fr1MmgVxIIzQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19936, version 1.1
Category:	downloaded
Size (bytes):	19936
Entropy (8bit):	7.969635209849544
Encrypted:	false
SSDEEP:	384:mvNCb8Eb+tS9nAIRMeC4J4h4Il7xtUOTCBGt+GXn/TUnOPgdGRhBg9r:Y4zbwTiMedJNIhkGbXn/TUnS+2hS9r
MD5:	E9DBBE8A693DD275C16D32FEB101F1C1
SHA1:	B99D87E2F031FB4E6986A747E36679CB9BC6BD01
SHA-256:	48433679240732ED1A9B98E195A75785607795037757E3571FF91878A20A93B2
SHA-512:	D1403EF7D11C1BA08F1AE58B96579F175F8DD6A99045B1E8DB51999FB6060E0794CFDE16BFE4F73155339375AB126269BC3A835CC6788EA4C1516012B1465E75
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOkCnqEu92Fr1MmgVxIIzQ.woff
Preview:	wOFF.....M.....GDEF.....G...d....GPOS.....hGSUB.....7b..OS/2.....R...`s.#.cmap.....L....cvt .....H...H.2..fpgm.....3...._...gasp...0..... ....glyf...<..;...n..e..hdmx..G<...i.....head..G....6...6.G..hhea..G.....$...`hmtx..H....M.....Wd^loca..JP.....maxp..L,... ... .name..LL.....x..9.post..M ..... .m.dprep.. M4.....+6.x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R.....2.x.....[....#N..m.m.m.mfm....SP..NuM..9]..=.U..!...[.....w...|.....^p....H.....;..)..... .;..EoDo.. ..E.E.D...`.0.GG.aA.H.V.Mx\xA...../..d3.Eb_.J...R.^v.....\^ob.}.z..k.x).v$f$..O)+.2..*....y}6`C6b.6cs...l.....!.....<..|.|..|..|..|.|....o....l%.4.L.SI.&C.6..!`...{...c..\.J.(.2.C....V.A ..?.M<nG.....v..m.;..R.C..aj.H...=..{.>.:.....}i_Y.....:....o.&k..KY.2..6k....i]..{,.p}../.....VO3.o].fJ....R-TZ..;...RN..&V...C...3.?.....&..z.s&.D....r,.I...t.R..a$k..Mm..Y.U...+b.%kQ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\KFOlCnqEu92Fr1MmSU5fBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19916, version 1.1
Category:	downloaded
Size (bytes):	19916
Entropy (8bit):	7.96782347282656
Encrypted:	false
SSDEEP:	384:JiNCb8EbT1rG/3rjJmQ8uLc5ZiRE5HWSiPTI45tKVr6+F7gLLdz:k4zbM3rjEQ8uQPiRERWSGIWtKVrWJ
MD5:	A1471D1D6431C893582A5F6A250DB3F9
SHA1:	FF5673D89E6C2893D24C87BC9786C632290E150E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\KFOlCnqEu92Fr1MmSU5fBBc-[1].woff	
SHA-256:	3AB30E780C8B0BCC4998B838A5B30C3BFE28EDEAD312906DC3C12271FAE0699A
SHA-512:	37B9B97549FE24A9390BA540BE065D7E5985E0FBFBE1636E894B224880E64203CB0DDE1213AC72D44EBC65CDC4F78B80BD7B952FF9951A349F7704631B903C6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmSU5fBBc-.woff
Preview:	wOFF.....M.....GDEF.....G...d....GPOS.....hGSUB.....7b..OS/2.....R...`t.#.cmap.....L....cvt .....X...X/...fpgm.....4.....".gasp...@..... ....glyf...L..:...j...w.hdmx..F....d.....head..GD...6...6.Y.ihhea..G|.....$...vhmtx..G....k.....\].loca..J.....g.L.maxp..K.... ... ...\name..L.....|..9.post..L..... .m.dprep..L.....: z/.Wx...1..P.....PB..U.=I.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R.....2.x.....[....#N..m.m.m.mfm....SP..NuM..9]..=.U..!...[.....w...|.....^p....H.....;...).....;..EoDo....E.E.D.. .`.0.GG.aA.H.V.Mx\xA...../..d3.Eb_.J...R.^v.....\^ob.}.z..k.x).v$f$..O)+.2..*....y}6`C6b.6cs...l.....!.....<..|..|..|..|.|....o....l%.4.L.Sl.&C.6..!`...{...c..\.J.(.2.C....V.A..?.M<nG. .....v..m.;..R.C..aj.H...=..{.>.:.....}i_Y.....:....o..&k..KY.2..6k....i]..{,.p}../.....VO3.o].fJ....R-TZ..;...RN..&V...C...3.?.....&..z.s&.D....r,.I...t.R..a$k..Mm..Y.U...+b.%kQ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\bscframe[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with no line terminators
Category:	dropped
Size (bytes):	15
Entropy (8bit):	3.906890595608518
Encrypted:	false
SSDEEP:	3:PouVn:hV
MD5:	FE364450E1391215F596D043488F989F
SHA1:	D1848AA7B5CFD853609DB178070771AD67D351E9
SHA-256:	C77E5168DFFDA66B8DC13F1425B4D3630A6656A3E5ACF707F4393277BA3C8B5E
SHA-512:	2B11CD287B8FAE7A046F160BEE092E22C6DB19D38B17888AED6F98F5C3E936A46766FB1E947ECC0CC5964548474B7866EB60A71587A04F1AF8F816DF8AFA221E
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\m=sy71,wg1P6b[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	3653
Entropy (8bit):	5.52166833644869
Encrypted:	false
SSDEEP:	96:xR2Mmp3QHFoHTLhKHxDIHF2PzuFW0NQZB:0QHF2KaF2PzukGE
MD5:	47E86314795B1738D16CFAE07E5CD416
SHA1:	2B82318F4FC1537CB1B163C786122BA6267D7F15
SHA-256:	3C988B5F72D46DD5DF476AB7E85398BD441DA816B32DF6E0B10B8404A2D8CB59
SHA-512:	D4740A26C8FC9029E12A5D2FEE4CCF1FE5D1970F71AC84340E4A6C26D70305450C055E848437DCA1403262DAD4EBC54EA3047B7A2A47E083CE9B1406D20400E
Malicious:	false
Reputation:	low
Preview:	this._G=this._G||{};(function(_){var window=this;.try{._.k("sy71");_.e4a=_.pt("dcnbp");_.f4a=_.pt("iFFCZc");_.g4a=_.pt("EDR5Je");_.h4a=_.pt("Rld2oe");_.i4a=_.pt("FzgWvd");./*.. Copyright 2018 Google Inc... Permission is hereby granted, free of charge, to any person obtaining a copy. of this software and associated documentation files (the "Software"), to deal. in the Software without restriction, including without limitation the rights. to use, copy, modify, merge, publish, distribute, sublicense, and/or sell. copies of the Software, and to permit persons to whom the Software is. furnished to do so, subject to the following conditions:.. The above copyright notice and this permission notice shall be included in. all copies or substantial portions of the Software... THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR. IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,. FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL T

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\4UaGrENHsxJlGDuGo1OIlL3Owpg[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26180, version 1.1
Category:	downloaded
Size (bytes):	26180
Entropy (8bit):	7.9847487601205405
Encrypted:	false
SSDEEP:	768:axmLo3N7711ZHlB8N6yt/DvXjXjmDNzv6:bLodN78li7jKJv6
MD5:	4F2E00FBE567FA5C5BE4AB02089AE5F7
SHA1:	5EB9054972461D93427ECAB39FA13AE59A2A19D5
SHA-256:	1F75065DFB36706BA3DC0019397FCA1A3A435C9A0437DB038DAAADD3459335D7
SHA-512:	775404B50D295DBD9ABC85EDBD43AED4057EF3CF6DFCCA50734B8C4FA2FD05B85CF9E5D6DEB01D0D1F4F1053D80D4200CBCB8247C8B24ACD60DEBF3D739A4CF0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\4UaGrENHsxJlGDuGo1OIlL3Owpg[1].woff	
IE Cache URL:	http://https://fonts.gstatic.com/s/googlesans/v14/4UaGrENHsxJlGDuGo1OIlL3Owpg.woff
Preview:	wOFF.....fD.....GDEF.....\.....QGPOS.....#..+...QGSUB.....y.....m.OS/2...|...U...`h...cmap.....~n...cvt .....y.....fpgm.....uo..gasp.....glyf.... ..=...m...5head..Z....6...6..'.hhea..Z.... ...$.0.5hmtx..[.....).loca..]....y.....K.6maxp..`H.. ... .=..name..`h.....r.i6Ppost..a.....i]\prep..d....p..... ..x.U....Q.F..=#.0ZD.@@<..... "...Zp....+.c.f...).>Z.bm.Om..?...\\.zi.f.^b...[y/.....x..Z..+..=Z...~.....0.8....r.\|...=s&oG....q.Fg...Y...:Wc..>..p..p....).....{.aX..}.?.k... .....N.=.c.Do.....~2.=.i$....0..>..!.'v.....q. ...>>.....o....30..0.w..|hR&mrf....,.Y.....%<..0.#.~...._a.c.....K.z...H1..u.2.Y_..0.9..`.,.:.=(.N~..*.a.<.D=....*.V....\..>./.B.`iE..A9.S.|?.g).Rj..8Q...h.y.G.^.kx.o.....(...#....9... ,4I8...7..o.I|@x..1.>'...H.m..$.yp..f..%..F$0.0.I.1...WR...E..8?a..|".....A.(...ZJ.q.K|...S.1..ht.ck....e...T.Zs,W..0..%.i.R...Ku.K.y.....j.RD..~..dpsh.fc.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\KFOlCnqEu92Fr1MmWUlfBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19888, version 1.1
Category:	downloaded
Size (bytes):	19888
Entropy (8bit):	7.96899630573477
Encrypted:	false
SSDEEP:	384:0c6bX9TSzYzCrQH+qXM6C0ouF0xcYye+5x/U3S0X5v+obEgm:0cCV8GuPVyzx/MS0X5v+oI/
MD5:	CF6613D1ADF490972C557A8E318E0868
SHA1:	B2198C3FC1C72646D372F63E135E70BA2C9FED8E
SHA-256:	468E579FE1210FA55525B1C470ED2D1958404512A2DD4FB972CAC5CE0FF00B1F
SHA-512:	1866D890987B1E56E1337EC1E975906EE8202FCC517620C30E9D3BE0A9E8EAF3105147B178DEB81FA0604745DFE3FB79B3B20D5F2FF2912B66856C38A28C07EE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmWUlfBBc-.woff
Preview:	wOFF.....M.....GDEF.....G...d....GPOS.....GSUB.....7b..OS/2.....P...`u.#.cmap...0.....L....cvt .....H...H+~..fpgm...(...3...._...gasp...\..... ....glyf...h...:q..i..+ Ohdmx..F....f.....head..GD...6...6...\hhea..G|.....$.&..hmtx..G....d.....E#loca..J.....\s@.maxp..K.... ... .name..K.....~..9.post..L..... .m.dprep..L.....)* v60x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R.....2.x...pfK.G...1.c>..`9..m<+;..m.x...bg.M.T...O.....l...XU.../{.[_..W....c._..72.. ." z.+..F.....&.&...`e..T]. ....K=..K2S....q..d...xf.$~i..$?.d..dU.....@R-/LMO-J6...[]..Z..O.C_."lf..d....fS....$d.G>eL`....Tf1.....9.c>..`1.TR..x./d-.....q.....7....{...v.....!.....1.QG=.4.D3-..F;=..1'.'q.rw. ..9..e!.....Q....f.....qV.n.h.V.Z]..B..C.[B...V.....v...o.w.{...w..zRO.i=..._.....-.m....].=...[...(1.(.#.....O0/.0?..04rL.G.9.....i6..l..|.(o.....|$,..{|&|....YJ...x.e8B.#..t;R8.{+....\=.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\ServiceLogin[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	1667445
Entropy (8bit):	5.822805413260418
Encrypted:	false
SSDEEP:	12288:CQK38hJxla9fIjTWkJijYt+rUZYfiSOadRVFRABCruTpwY3cZ3MPhs2Y7:Pxla9QjTTCY4oSiShbRFewY3ci5Q
MD5:	F502815C5C9CBD0728302939C82A023A
SHA1:	C9536E5BBDF7A08C7C40DAB9EB848C4E8F1829B7
SHA-256:	4084DB6950D711D4581AFB267CDBBC2D2BBDAD7ADA751B70136027759C5CAEFB
SHA-512:	9150997E81847D9D6D804C30E3CFA8A03131AA573B08D8B7CC73A75BB23554B7252DF13F41595658FD6715CCD8E2DD694C0A35DC7BA8BED6AE4F3FA1D3E66C 8
Malicious:	false
Reputation:	low
Preview:	<!doctype html><html lang="de" dir="ltr"><head><base href="https://accounts.google.com/"><script data-id="_gd" nonce="+b/CKG8BYYJ1JbGUDKE4Aw">window.W IZ_global_data = {"Mo6CHc":-8960914142729793713,"OewCAd":"%.@.\"xsrf\",null,[\"\"]\n,\"AFoagUVpyVo7zX6Ub8_yiDBOlYDI00isjQ:1624378254171\"]\n","Qzxixc" :"S1896270411:1624378254149906","thykhd":"AKH95esMYvaToslfwigpi9-C5ENk7Ilhc9uA8Snma0FuqwUKMGrFRmnp24NKNTyP8t6-7nyw5hRsk6-8zP8AatFE N5h7QI_gMG5udipc1stK6MtDSm4\u003d","w2btAe":"%.@.null,null,\"\",false,null,null,true,false]\n"};</script><meta charset="utf-8"/><meta http-equiv="X-UA-Compatible" content="IE=edge"/><link rel="shortcut icon" href="//www.google.com/favicon.ico"/><noscript><meta http-equiv="refresh" content="0; url=https://accounts.googl e.com/ServiceLogin?continue=https%3A%2F%2Ffeedburner.google.com%2Ffb%2Fa%2Fmyfeeds&rip=1&nojavascript=1&service=feedburner&i fkv=AU9NCcyuYS64lStWUgN71rf02va9gVGKhjYlrnT7xY3GNvgCzmBGZe_cN_TE0ctZuI8l28lR4IwH"><style nonce="4UbYklutz3q+gN

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 2 icons, 16x16, 32 bits/pixel, 32x32, 32 bits/pixel
Category:	downloaded
Size (bytes):	5430
Entropy (8bit):	3.6534652184263736
Encrypted:	false
SSDEEP:	48:wlJct3xIAxG/7nvWDtZcdYLtX7B6QXL3aqG8Q:wlJct+A47v+rcqlBPG9B
MD5:	F3418A443E7D841097C714D69EC4BCB8
SHA1:	49263695F6B0CDD72F45CF1B775E660FDC36C606
SHA-256:	6DA5620880159634213E197FAFCA1DDE0272153BE3E4590818533FAB8D040770
SHA-512:	82D017C4B7EC8E0C46E8B75DA0CA6A52FD8BCE7FCF4E556CBDF16B49FC81BE9953FE7E25A05F63ECD41C7272E8BB0A9FD9AEDF0AC06CB6032330B096B3702 563
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/favicon.ico

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\favicon[1].ico	
Preview:	..... .h...&... ....(..... ....0.....v.].X.:.X.:r.Y..... .....q.X.S.4.S.4.S.4.S.4.S.4...X.....0.....q.W.S.4.X.:.....J...A...g.....K.H.V.8.....F..B.....,..... .....B.....B..B..B..B..B...u.....B..B..B..B..B...{.....5.....k.....7R..8F..... .....2.....Vb..5C..;I.....R^.....0.....Xc..5C..5C..5C..5C..5C..5C..lv.....]i..<J..:G..Zf..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\m=sy7g,sy7h,sy7i,sy7k,sy7l,sy9h,pwd_view[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	17015
Entropy (8bit):	5.601366295422354
Encrypted:	false
SSDEEP:	192:GYWJStYWjcLp4+y7rWyvs2PTKa2NgD74eFQJVEI2HNdy/D1VXqtLm6Gz2h92Icgi:wQtBcLYF5Ka22RQJVEISy/7flqhogowK
MD5:	05AC5EEC1972B65AB4308968B9448D22
SHA1:	86F3195ACBB3BD952722D2E4599E4CB3A77074BD
SHA-256:	A43E255BEC89B4460FB2FD26758B24A7B327962863AF75A4CB8B2FE3429BD01C
SHA-512:	89EDAD58A893E5B9BA4578F534E608A357B00CAC97761D93234B8BF61D7158654000239BE93E207B36B1127D4DDEA65F808D3921D61ACB177748D104DB50B365
Malicious:	false
Reputation:	low
Preview:	this._G=this._G||{};(function(_){var window=this;.try{._.k("sy7g");._.rT=function(){return"Andere Option w\u00e4hlen"};_.sT=function(){return"Code eingeben"};.._.m();..}catch(e){_._DumpException(e)}.try{._.k("sy7h");._.tT=function(){return(0,_.C)("Kontowiederherstellung")};_.uT=function(){return"Identit\u00e4t best\u00e4tigen"};.._.m();..}catch(e){_._DumpException(e)}.try{._.k("sy7i");._.W6a=function(){return"Passwort eingeben"};_.H("Rc","",0,function(){return"Falsches Passwort. Bitte noch einmal versuchen oder auf \u201ePasswort vergessen\u201c klicken, um das Passwort zur\u00fcckzusetzen.")});_.H("Sc","",0,function(){return"Passwort vergessen?"});.._.m();..}catch(e){_._DumpException(e)}.try{._.k("sy7k");._.vT=function(a,b){b=b&&(b.ia||b);var c=a.locale;a="";var d=c=_.As(_.ys("en,en-US,"),c+",");d&&(d=_.wF(b),d=_.G(null==d?null:d.getGivenName()));!d&&(d=!c)&&(d=_.wF(b),d=_.G(null==d?null:d.Pb()));return a=d?a+(c?"Hi "+_.wF(b).getGivenName():""+_.wF(b).Pb()):a+"Willkommen"};.._.m();..}c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\2F05QQI3.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT)
Category:	dropped
Size (bytes):	160
Entropy (8bit):	6.338565842886398
Encrypted:	false
SSDEEP:	3:Fttx12jexcoZyCaxFvf+mT2lZEdFs7e02MuYJx7weYUqA5dURt:Xtx1yZD+kRQ7X2MfYUqA5W7
MD5:	65679A994CB5C379C535C14B598E69F9
SHA1:	C6E481C6D49C3B504D30B0FA1CA9B57B05053D87
SHA-256:	CABC7FC601EB2A00A8BF61ACB5F6DEAF059305DDCE8196BD4721A87180E01F78
SHA-512:	2EC8D37EB12080ADC6D922BCD6111D1F9C0F086FC04778A0BCAC86F585A14FED08B3EE8093BD097636FB9A86640F67BAB4C1D784623D6323B93A5ED318CC70D
Malicious:	false
Reputation:	low
Preview:	.....put.R!.!>.v..e.)...E..y.y%9.6.....}.B'..H.'wg... [%e70PR.q...r..@.d.!6..\!...)...@1...b.\.:.G.. W7[%..$.D....T%...T.}G;=..@6...v8.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\4UabrENHsxJlGDuGo1OIlLU94YtzCwA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26412, version 1.1
Category:	downloaded
Size (bytes):	26412
Entropy (8bit):	7.982191465892414
Encrypted:	false
SSDEEP:	768:BXFxTA19K8CdHMT6KHQO8LWhHCWN1ekhzLS:9f29ZYMTwO8qh1nm
MD5:	142CAD8531B3C073B7A3CA9C5D6A1422
SHA1:	A33B906ECF28D62EFE4941521FDA567C2B417E4E
SHA-256:	F8F2046A2847F22383616CF8A53620E6CECDD29CF2B6044A72688C11370B2FF8
SHA-512:	ED9C3EEBE1807447529B7E45B4ACE3F0890C45695BA04CCCB8A83C3063C033B4B52FA62B0621C06EA781BBEA20BC004E83D82C42F04BB68FD6314945339DF2A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/googlesans/v14/4UabrENHsxJlGDuGo1OIlLU94YtzCwA.woff
Preview:	wOFF.....g,.....GDEF.....q.....GPOS.....%..+...RGSUB.....y.....m.OS/2.....U...`i`..cmap.....~n...cvt .....fpgm...@.....uo..gasp..... ..glyf.....>F..m>Q..head..[\...6...6..'.hhea..[.... ...$...3hmtx..[.....<'3loca..^l...{...._.{.maxp..`.... ... ....name..a.....V..4.post..a.....i]\prep..et.....^....x.D...Q...3..IX=D.@ @....@....."...}.....`.%.....x.....umW...g.WwO.....J..^?.Jci^N{.Nr..Jw@.n(.....t4....g...x.....6.E..8.....affff.0.B..&.L...B.Nzy..n.T.t~w&..%[.dYzzz.Oe" ..lE.....m..7[s}...[l..)..)... (H.A.@q.57..S.@.._..].*.j.-^N.R...'...]v.0..2n.6...~....X..xN.DN.T..b..*Q5.E.).,Ql.....M....6.P."..\|..*.tI5.....t..r.(...{M..T}..@.kbNP.I*.9-...=E.U'.{.....p\|.t..qJE.9...'...*...z...L./.....r nXQ.6.\|.....n.V.....K.?.G...<..<..Q.....C..K(s.PR.x\(..P@.P..z.DL.1.$*../.8A.8Q.r.Pr[e.Rt+~.}9.)E.'.U..z.G..G..OH/H...L.../..{S...EP.%.....o.....uN...'.}%..9.F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\CheckConnection[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	35944
Entropy (8bit):	5.4250766965476025
Encrypted:	false
SSDEEP:	384:PvRA/njbgtzhR/1PjSoXV2fmsxkuwGf6eDH2ge3TJXiWKsr4/FbUUjkyFtgKZDy5:PZLx7sqzGrrK3dXiW/rCAgBye37cd
MD5:	6F29FCC1070D2A54B3135DE5DC5EE813
SHA1:	BE4FBD119087F1E1C7C84D867AEB9056A6F1F7BD
SHA-256:	D1C51E9DA002BFAB702CE94A3FB84A30CDEAC33EEB03C725570CA87A9D2D9110
SHA-512:	DE996265DFE978875C8149CA326B24163E471A2311DBACE70F65F9B93516EF5033224F10E1154CAD39B6672922C633228F6F462E5AE94E0AE2665BF307D2A230
Malicious:	false
Reputation:	low
Preview:	<html><head><script nonce="W5Hlk870PvjMrDqNb09ZmQ">"use strict";this.default_AccountsDomaincookiesCheckconnectionJs=this.default_AccountsDomaincookiesCheckconnectionJs||{};(function(_){var window=this;.try{./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var n,p=function(a,b){if(Error.captureStackTrace)Error.captureStackTrace(this,p);else{var c=Error().stack;c&&(this.stack=c)}a&&(this.message=String(a));b&&(this.Y=b)},aa=function(a,b){a:{for(var c=a.length,d="string"===typeof a?a.split(""):a,e=0;e<c;e++)if(e in d&&b.call(void 0,d[e],e,a)){b=e;break a}b=-1}return 0>b?null:"string"===typeof a?a.charAt(b):a[b]},ca=function(a,b){b=ba(a,b);var c;(c=0<=b)&&Array.prototype.splice.call(a,b,1);return c},da=function(a,b){return null!==a&&b in a},fa=function(a,.b){for(var c,d,e=1;e<arguments.length;e++){d=arguments[e];for(c in d)a[c]=d[c];for(var f=0;f<ea.length;f++)c=ea[f],Object.prototype.hasOwnProperty.call(d,c)&&(a[c]=d[c])}},ha=function(a){q(a)},ka=functio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\m=n73qwf,MpJwZc,NpD4ec,SF3gsd,O8k1Cd,YLQSd,lCVo3d,o02Jie,rHjpXd,pB6Zqd,QLpTOd,otPmVb,rlNAl[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	2617
Entropy (8bit):	5.315909211489001
Encrypted:	false
SSDEEP:	48:x7aFuwAMt1AfyaCgGda5/ZLSSylzI5ECPetwPthLk7kv5pNEFn:xK/aFZL/11PswPtNk7kv5pKt
MD5:	D4ABDA400898A6A5BE25BB78C0622EC8
SHA1:	BCBE0279FC22749561D93A1DD3CDFF5C3229CF4D
SHA-256:	AC6A880909A7198C329747945CFD8D0E25457A3FCBF561B36668773F06E9D410
SHA-512:	44A449D5D9EEFA755C5AD6A74328BA95D0F38DCB4DBC5381FD9351A8C2FE5617112D56C69E50CC79161D020F401BF1802DED4E825AB22F08654F818F17C1AE4
Malicious:	false
Reputation:	low
Preview:	this._G=this._G||{};(function(_){var window=this;.try{._.k("n73qwf");.._.m();..}catch(e){._.DumpException(e)}.try{._.k("MpJwZc");.._.m();..}catch(e){._.DumpException(e)}.try{._.k("NpD4ec");.._.m();..}catch(e){._.DumpException(e)}.try{._.k("SF3gsd");.._.m();..}catch(e){._.DumpException(e)}.try{._.k("O8k1Cd");.._.m();..}catch(e){._.DumpException(e)}.try{._.k("YLQSd");._.at(_.lx);.._.m();..}catch(e){._.DumpException(e)}.try{._.k("lCVo3d");.._.m();..}catch(e){._.DumpException(e)}.try{._.k("o02Jie");.._.m();..}catch(e){._.DumpException(e)}.try{._.k("rHjpXd");.._.m();..}catch(e){._.DumpException(e)}.try{._.k("pB6Zqd");.._.m();..}catch(e){._.DumpException(e)}.try{._.k("QLpTOd");.._.m();..}catch(e){._.DumpException(e)}.try{._.k("otPmVb");._.z9=function(a){_.KC.call(this,a.Da)};_.x(_.z9,_.KC);_.z9.eb=_.KC.eb;_.z9.ta=_.KC.ta;_.Ev(_.hua,_.z9);.._.m();..}catch(e){._.DumpException(e)}.try{.var A9=function(a){_.y(this,a,-1,null,null)};_.x(A9,_.q);A9.prototype.Hb=function(){return _.r(this,7)};A9.pro

C:\Users\user\AppData\Local\Temp\~DF2D90F4100E2FE8B0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47634575158430514
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9loC9loy9lW4I2kZk3a:kBqoItr4saq
MD5:	B879099BA3253E38DE4C8FCC58CB5F75
SHA1:	1805BD0522C71C9AEDD926DE8AAE88570E60D354
SHA-256:	1EB0F5603B7AD7220A1A66BF6B2EEC086F96C9B91C355A0FB37AFA1A2E0512E2
SHA-512:	2A7BC223B29546103B5A6F06D876D7B13AE79C7395C19335AD6D60D3ACA4A5035D0A3D6517DCFC001120AC45F47DE6B60DA117C41A414ECD77BAFC49E934140
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFC13BC963B5A42CA7.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data

C:\Users\user\AppData\Local\Temp\~DFC13BC963B5A42CA7.TMP	
Category:	dropped
Size (bytes):	53201
Entropy (8bit):	0.7902942241640337
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+eYSbInaKavTFvsfR1kCg5UoFvsxURoFvsXoFvsSYgsS:kBqoxKAuqR+eYSbInJQTq1oJoAo1t
MD5:	CAEA2FFE3595F683B682905C15BB1318
SHA1:	FE7406A25ABE8DD006497B8FB9CD5EEE8783FEC7
SHA-256:	5A4C064CAA6A9CD7E9B3797449F8257C723CDA8AC81247BD918F397BB2A1CA09
SHA-512:	848BD80466DAAF831F7112205324114763F6EF8033B973A5E6AF2F1CD616D330D33D53FA28D3023870FA47C4854661471487DC84CE2EE0D0BAF83ACC5CBC678
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFCD36760A8D17F84A.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.41687881123205234
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAVOLNSu:kBqoxxJhHWSVSEabVO
MD5:	27538E13BEDB88AB0FCCA548A0FD04F6
SHA1:	05F2FD78A7E012CA1ECD8652B82405C820A47ED8
SHA-256:	AB466919C797AB5DB64FBB996E55EFFEAACB3804D19E85DE73AE2F15E64DC263
SHA-512:	ECF837DF440762ED9DA1F9337DB332BFB8F1BED5D5F913131DB1B080AE60402DA392887B31604DDD9FB2F792EED770348496A5025550DC7EF60FEB24461A9B3
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

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 22, 2021 18:10:57.119240999 CEST	192.168.2.4	8.8.8.8	0x756b	Standard query (0)	accounts.youtube.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 22, 2021 18:10:57.189645052 CEST	8.8.8.8	192.168.2.4	0x756b	No error (0)	accounts.youtube.com	www3.l.google.com		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5424 Parent PID: 800

General

Start time:	18:10:33
Start date:	22/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7cdbd0000
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

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 4552 Parent PID: 5424

General

Start time:	18:10:33
Start date:	22/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5424 CREDAT:17410 /prefetch:2
Imagebase:	0x170000
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 Show Windows behavior

Registry Activities Show Windows behavior

Disassembly