ID: 323228
Cookbook: browseurl.jbs
Time: 15:09:03
Date: 26/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

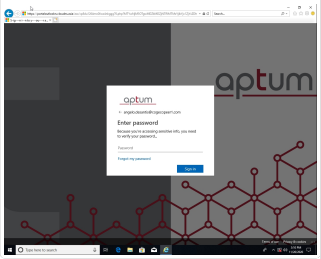
Analysis Report http://gomterly.tk/nomter/YW5nZWxvLm…

Overview

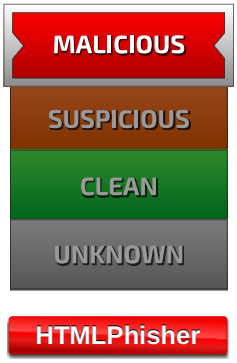
General Information

Sample URL:	http://gomterly.tk/nomter/YW5nZWxvLmRlc2FudGlzQGNvZ2Vjb3BlZXIxLmNvbQ==
Analysis ID:	323228

Most interesting Screenshot:



Detection

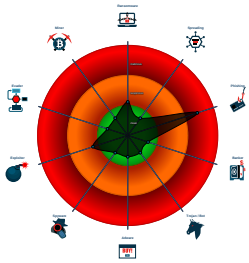


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Phishing site detected (based on fav…
- Yara detected HtmlPhish_10
- Allocates a big amount of memory (p…
- HTML body contains low number of …
- HTML title does not match URL
- Invalid T&C link found

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 2976 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 2944 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2976 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

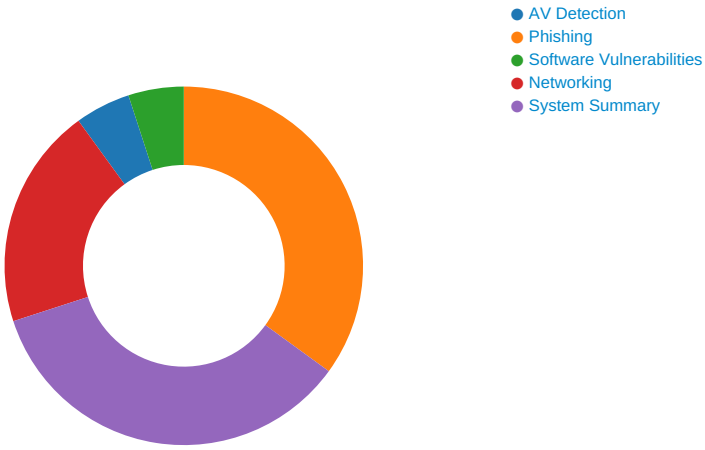
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\cp8du1264mo0liwz4nkggg76[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Phishing:

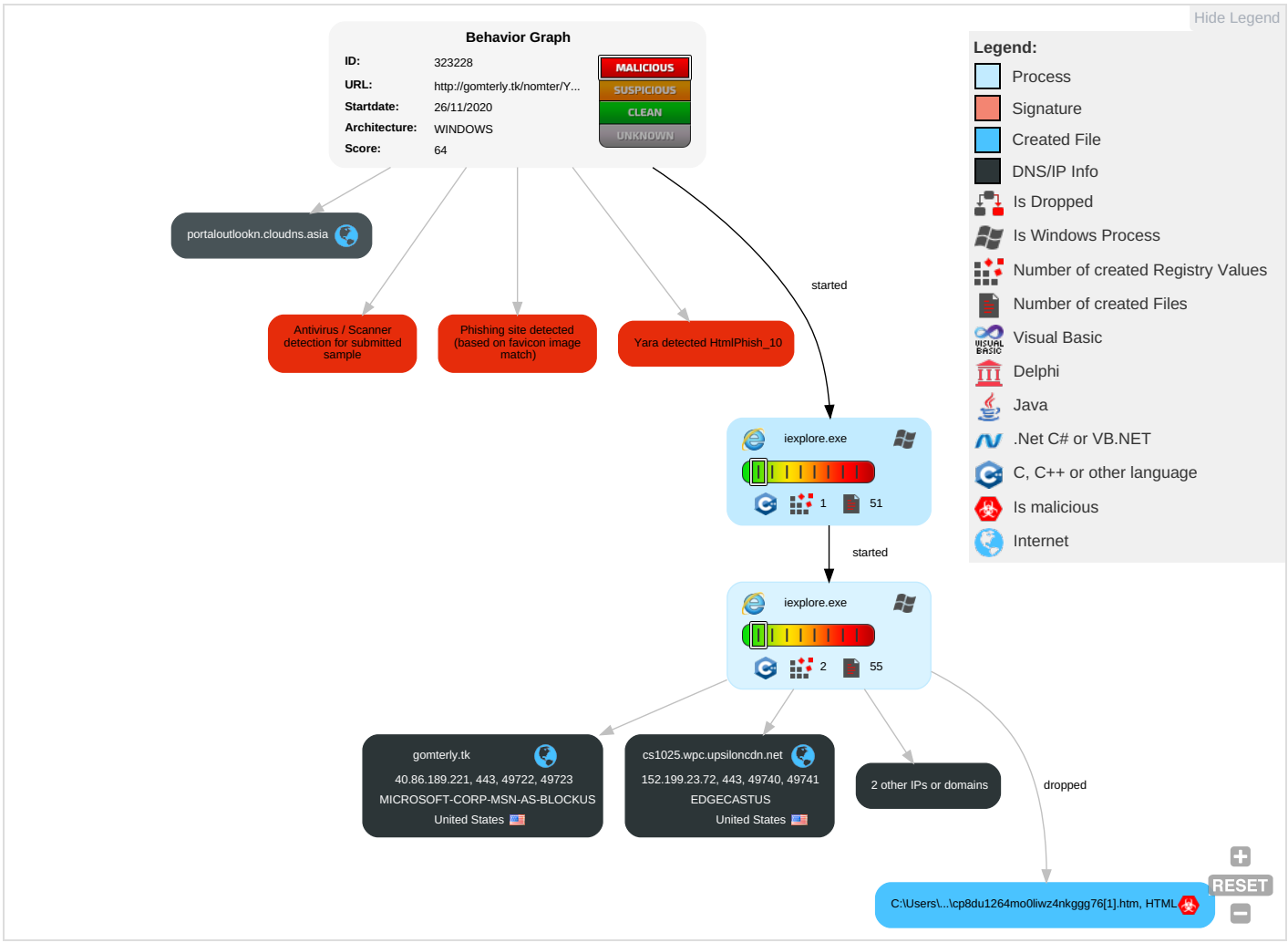
Phishing site detected (based on favicon image match)

Yara detected HtmlPhish_10

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impac
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partiti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	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 Lockc
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Extra Window Memory Injection 1	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		Carrie Billing Fraud

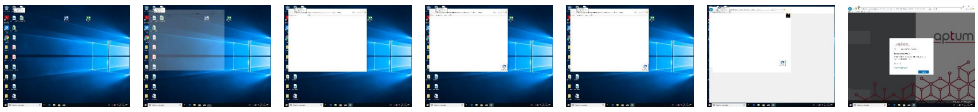
Behavior Graph

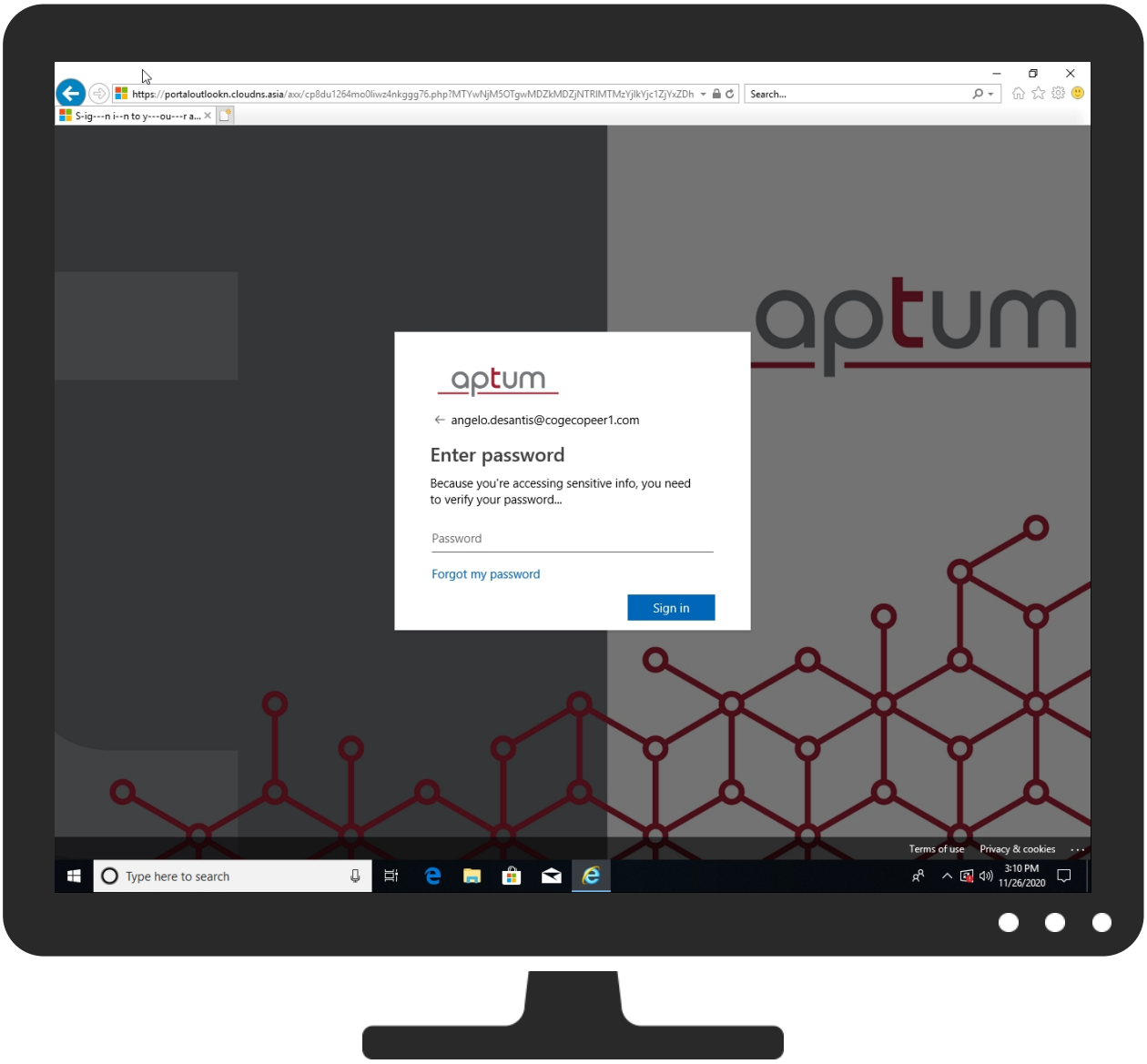


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://gomterly.tk/nomter/YW5nZWxvLmRlc2FudGlzQGNvZ2Vjb3BlZXIxLmNvbQ==	0%	Avira URL Cloud	safe	
http://gomterly.tk/nomter/YW5nZWxvLmRlc2FudGlzQGNvZ2Vjb3BlZXIxLmNvbQ==	100%	SlashNext	Fake Login Page type: Phishing & Social usering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://aadcdn.msauthimages.net/dbd5a2dd-vvz27-qbah61uolzvyjrsjirzzc1kxvx6nwaiet9-sg/logintenantbran	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://portaloutlookn.cloudns.asia/axx/proc?csrftoken=MTYwNjM5OTc5NTZkMDZjNTRlMTMzYjlkYjc1ZjYxZDhiY	0%	Avira URL Cloud	safe	
http://gomterly.tk/nomter/YW5nZWxvLmRlc2FudGlzQGNvZ2Vjb3BlZXIxLmNvbQ==Root	0%	Avira URL Cloud	safe	
http://https://portaloutlookn.cloudns.asia/axx/lib/img/favicon.ico	0%	Avira URL Cloud	safe	
http://https://portaloutlooknter/YW5nZWxvLmRlc2FudGlzQGNvZ2Vjb3BlZXIxLmNvbQ==.cloudns.asia/axx/proc?csrftok	0%	Avira URL Cloud	safe	
http://https://portaloutlookn.cloudns.asia/axx/cp8du1264mo0liwz4nkggg76.php?MTYwNjM5OTgwMDZkMDZjNTRlMTMzYjl	0%	Avira URL Cloud	safe	
http://https://portaloutlookn.cloudns.asia/axx/lib/img/favicon.ico~(	0%	Avira URL Cloud	safe	
http://https://portaloutlookn.cloudns.asia/axx/?angelo.desantis	0%	Avira URL Cloud	safe	
http://https://portaloutlookn.cloudns.asia/axx/lib/img/favicon.ico~	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
portaloutlookn.cloudns.asia	40.86.189.221	true	false		unknown
gomterly.tk	40.86.189.221	true	false		unknown
cs1025.wpc.upsiloncdn.net	152.199.23.72	true	false		unknown
aadcdn.msauthimages.net	unknown	unknown	false		unknown

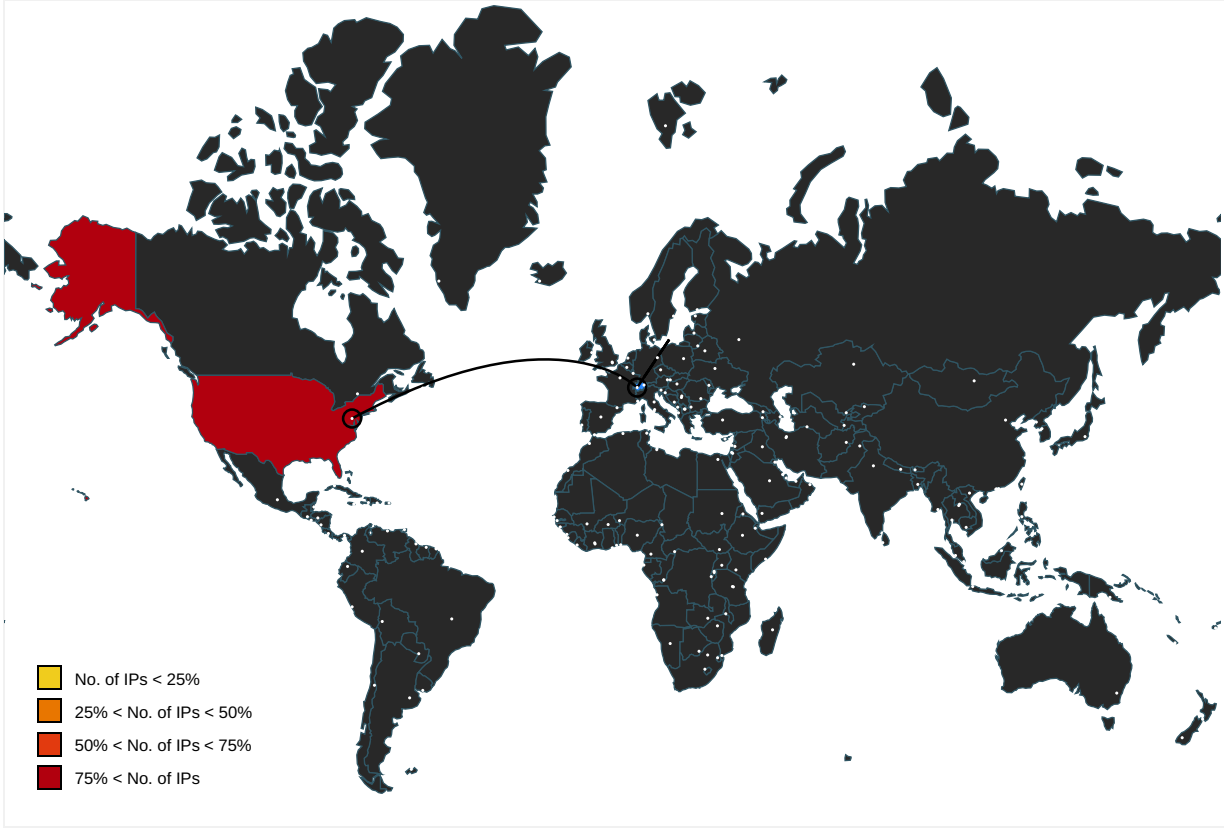
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://portaloutlookn.cloudns.asia/axx/cp8du1264mo0liwz4nkggg76.php?MTYwNjM5OTgwMDZkMDZjNTRlMTMzYjlkYjc1ZjYxZDhiY2U4OTBlZWU4OTcyNmFkYTE3NDUxYTlmMDVmNDdhZjI3YjM3NjJlOTNhMDhkYjgwZg==&data=YW5nZWxvLmRlc2FudGlzQGNvZ2Vjb3BlZXIxLmNvbQ==	true		unknown
http://gomterly.tk/nomter/YW5nZWxvLmRlc2FudGlzQGNvZ2Vjb3BlZXIxLmNvbQ==	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aadcdn.msauthimages.net/dbd5a2dd-vvz27-qbah61uolzvyjrsjirzzc1kxvx6nwaiet9-sg/logintenantbran	cp8du1264mo0liwz4nkggg76[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://portaloutlookn.cloudns.asia/axx/proc?csrftoken=MTYwNjM5OTc5NTZkMDZjNTRlMTMzYjlkYjc1ZjYxZDhiY	~DFEA39457A0CB7C84C.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	KFOlCnqEu92Fr1MmYUtfBBc9[1].ttf.2.dr, KFOmCnqEu92Fr1Mu4mxP[1].ttf.2.dr, KFOlCnqEu92Fr1MmEU9fBBc9[1].ttf.2.dr	false		high
http://gomterly.tk/nomter/YW5nZWxvLmRlc2FudGlzQGNvZ2Vjb3BlZXIxLmNvbQ==Root	{7BDBF09E-303C-11EB-90E5-ECF4BB2D2496}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://portaloutlookn.cloudns.asia/axx/lib/img/favicon.ico	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://portaloutlooknter/YW5nZWxvLmRlc2FudGlzQGNvZ2Vjb3BlZXIxLmNvbQ==.cloudns.asia/axx/proc?csrftok	{7BDBF09E-303C-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false	• Avira URL Cloud: safe	low
http://https://portaloutlookn.cloudns.asia/axx/cp8du1264mo0liwz4nkggg76.php?MTYwNjM5OTgwMDZkMDZjNTRlMTMzYjl	{7BDBF09E-303C-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://portaloutlookn.cloudns.asia/axx/lib/img/favicon.ico~(	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://portaloutlookn.cloudns.asia/axx/?angelo.desantis	YW5nZWxvLmRlc2FudGlzQGNvZ2Vjb3BlZXIxLmNvbQ==[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://portaloutlookn.cloudns.asia/axx/lib/img/favicon.ico~	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
40.86.189.221	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
152.199.23.72	unknown	United States		15133	EDGECASTUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323228
Start date:	26.11.2020
Start time:	15:09:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://gomterly.tk/nomter/YW5nZWxvLmRlc2FudGlzQGNvZ2Vjb3BlZXIxLmNvbQ==
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:	5
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@3/27@4/2

Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): ielowutil.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 104.108.39.131, 52.255.188.83, 172.217.168.68, 216.58.215.227, 172.217.168.3, 51.132.208.181 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, arc.msn.com.nsatc.net, fonts.gstatic.com, arc.msn.com, e11290.dspg.akamaiedge.net, skypedataprdcoleus17.cloudapp.net, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, aadcdn.azureedge.net, aadcdn.ec.azureedge.net, www.google.com, watson.telemetry.microsoft.com, www.gstatic.com, skypedataprdcolwus16.cloudapp.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\DOMStore\UM9GSJ8J\www.google[1].xml	
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):	403
Entropy (8bit):	5.075057296488567

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\UM9GSJ8J\www.google[1].xml	
Encrypted:	false
SSDEEP:	12:JUAXgIIiS/Q5yrUAXgIIiS/Q5L4EyWPw5yrUA4EyWPw5U:yyQ5GUyQ5Bo5GUeo5U
MD5:	8F738C8357366341E42E3F635C3EAB8F
SHA1:	BEF0D2AE668ED89AE68F244BBDE050F0367CF8C7
SHA-256:	68D249AA036F6DB2A37228DDAFA960AF3B7EA9D9151B5CBF7A7D4B708FAABD9A
SHA-512:	D357CBB69C0FE2BEFE278AD3B8FFBB5400A3F3CC1871AE5A52D91B459DC522DC9D6748E1ED5DF2F15B4DA1EE1146624FF63E65ABAA15B01C45820E560AADEC9F
Malicious:	false
Reputation:	low
Preview:	<root><item name="rc::d-1606432197568" value="MWNrczF4Zm9nZGtvZw==" ltime="1110144976" htime="30852169" /></root><root><item name="rc::d-1606432197568" value="MWNrczF4Zm9nZGtvZw==" ltime="1110144976" htime="30852169" /><item name="rc::a" value="YTFjem0wbjc1MWt5" ltime="1110504976" htime="30852169" /></root><root><item name="rc::a" value="YTFjem0wbjc1MWt5" ltime="1110504976" htime="30852169" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{7BDBF09C-303C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8557716546968341
Encrypted:	false
SSDEEP:	96:rhZ6Za2L9WotmAfJx11MUtTQHR3+fyx0lX:rhZ6Za2L9WothfJdMM8ufycX
MD5:	68E74A5B458E909758ACAC6181C6F760
SHA1:	09ABE50B9739EFCF7A869A2486F1ADEDF39F0C45
SHA-256:	9EE7968C901F0D41F247F0ECB1397BBABC398265CC143218CD718E3688C85F0E
SHA-512:	AD9433C157A7DC7F5996B29DB16B8214C02FC9FAE439DD35359A58E29CF3EBDC1A83B0C076F0B533FDDACDFB81976569EB7F6D496143C425FDFAFEE17AC5FD8
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\{7BDBF09E-303C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	53064
Entropy (8bit):	2.756069796552991
Encrypted:	false
SSDEEP:	384:rtFzbRhgIVLS3KZg5euFC0+mw1AjjtYvmnQQ681AjZFg+5xvYPZH7FqbA:NS5euC0DJjomnQQI09gU
MD5:	8AB8134430CD7AC7181054296B323C2D
SHA1:	CA2AD04C7E11FA803885A47426AB7A50CEAC9018
SHA-256:	1D898F9C3C55E170071D0CA32E73EFAD5FEFABF3F664C37C61C330B3433AA17C
SHA-512:	4136D270B1E35748F75E1C31AE71A7C05C0BA068B98A126C19F0FF1F142D2D642E7A63CB777712ED1032B4B693ACBF878305B5D85FC958716F5273D04DC494FF
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\{85D741D5-303C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5649689956788024
Encrypted:	false
SSDEEP:	48:IwbGcpreGwpaEG4pQsGrapbSbrGQpKpG7HpRpsTGIpG:rBZWQ06qBSbFAITp4A
MD5:	71071EBEB0FAA3AA4258AFB7B35420FD
SHA1:	8CC3C48704A2588841946E6054A83B026F2BB2AB
SHA-256:	743D61B64D233BFF906EFA25FE783F357B94ECFF577682AC8C378976D17F0900
SHA-512:	DD1085F03AA5CF172E458892954870558AB6768ECB945D1C2C123B3575254B6612947791A04C443C25C62C54B232AEB4BED4010941F9C0DF3B361678B3255DF6

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{85D741D5-303C-11EB-90E5-ECF4BB2D2496}.dat	
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y.. ....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\wlm7n14\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	18140
Entropy (8bit):	3.0819883770771144
Encrypted:	false
SSDEEP:	48:S7VeE/h7VeE/W7VeE/+7VeE/tgyyyyyyyyyyyyyyh7VeE/Dy7VeE/GQQQQQt:SFa6JyCQQQQQt
MD5:	2181661F53D5562196E30FDBCCB27BFD
SHA1:	687FE0A3D86052821C23F4EEAE42007DB20CFC03
SHA-256:	923332BB585E17975EC4E6CC8C7FF67F85AA41AEB8A4726260ECFC28AC12E3EB
SHA-512:	D29C77E4005B4E5E50FAED166FE0864342B9AC28EFBDA4AF123EE66EEC4CF07ED4899CC335EACE1D5F7139EF1F1769E5342E510F2D722FACC5CA6390E34391 C8
Malicious:	false
Reputation:	low
Preview:	;.h.t.t.p.s.:././.p.o.r.t.a.l.o.u.t.l.o.o.k.n...c.l.o.u.d.n.s...a.s.i.a./.a.x.x./.l.i.b./.i.m.g./.f.a.v.i.c.o.n...i.c.o.~(................h(......(....................(....................................."P....................... ....""""""""""""""""""""""""""""""" ...33333333333333333333333333333333""""""""""""""""""""""""""""""" ...33333333333333333333333333333333""""""""""""""""""""""""""""""" .. .33333333333333333333333333333333""""""""""""""""""""""""""""""" ...33333333333333333333333333333333""""""""""""""""""""""""""""""" ...33333333333333333333333333333333" """"""""""""""""""""""""""""""" ...33333333333333333333333333333333""""""""""""""""""""""""""""""" ...33333333333333333333333333333333""""""""""""""""""""""""""""""" ...333333333 33333333333333333333333""""""""""""""""""""""""""""""" ...33333333333333333333333333333333""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"""""""""""""""" """"""""""""""" ...33333333333333333333333333333333""""""""""""""""""""""""""""""" ...333333333333

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 6 icons, 128x128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsLsQZp:nfgyyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://portaloutlookn.cloudns.asia/axx/lib/img/favicon.ico
Preview:	..............h(..f...HH...........(..00......h....6.. ....=...............@..........(....A..(....................(....................................."P...""""""""""""""""""""""""""""""" ...3 33333333333333333333333333333333""""""""""""""""""""""""""""""" ...33333333333333333333333333333333""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"""" """"""""""""""""""""""""""""""" ...33333333333333333333333333333333""""""""""""""""""""""""""""""" ...33333333333333333333333333333333""""""""""""""""""""""""""""""" ...33333333333 3333333333333333333333""""""""""""""""""""""""""""""" ...33333333333333333333333333333333""""""""""""""""""""""""""""""" ...33333333333333333333333333333333""""""""""""""""""""""""""""""" """"""""" ...33333333333333333333333333333333""""""""""""""""""""""""""""""" ...33333333333333333333333333333333""""""""""""""""""""""""""""""" ...3333333333333333333333 333333333""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"""""""""""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\recaptcha__en[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	343493
Entropy (8bit):	5.689500475116669
Encrypted:	false
SSDEEP:	6144:LD7O+JwNJ16l1rwc30d+FODzS77l5UkR6tmx:LLQ1EMrdpSHl5U3tmx
MD5:	E28E6938C382A88686493D368DE3F7F6
SHA1:	B268A8EAF2BF2BACA9D0E5AA816FF63970AEEA6A
SHA-256:	14A2806A256579773A3680E21459DEA7827D002104C6336856E0BEF9A39BE0C9
SHA-512:	93FEF84110208359642D1FD5B6FDB4E5792B79F27C40FCCD64AFC304E85520C6868F7220522F2F54876749CC1978560A1E7157318BD9206BD27871F8E243604A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/recaptcha/releases/UFwvoDBMjc8LiYc1DKXiAomK/recaptcha__en.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\recaptcha__en[1].js	
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var T=function(){return[function(Q,n,y,p,N,H){return(Q-1)%(((Q-(N=[11,33,7],N[2]))%N[0]||(yR.call(this),this.C=[]),(Q+N[2])%10)||!n.l||(n.F=y,n.l.onmessage=M(n.S,n)),N[0])||!p||(y.K?K[21](N[1],y.K,p)||y.K.push(p):y.K=[p],K[23](13,"7",n,y,p)),H},function(Q,n,y,p,N,H,k,c){if(!(((c=[null,11,43],Q)>>2)%c[1])){if((this.C=(this.P=(jx.call(this),n)||0,y)||10,this.P)>this.C)throw Error("[goog.structs.Pool] Min can not be greater than max");this.D=((this.F=new (this.l=new nj,pj),this).delay=0,c)[0],this.FR()}if(!((Q<<.((Q>>(3==((Q|2)&15)&&(N={},p=void 0===p?{}:p,w(T[5](c[2],n,Na),function(X,D,V){D=Na[X],D.zb&&(V=p[D.Z()]||this.get(D))&&(N[D.zb]=V)},y),k=N),1))%5||(N=r[37](57,n)(),k=q[27](13,y,p,N)),2))%14))a:{if((H=g[0](90,9,y),H).defaultView&&H.defaultView.getComputedStyle&&(N=H.defaultView.getComputedStyle(y,c[0]))){k=N[p]||N.getPropertyValue(p)||n;break a}k=n}return k},function(Q,n,y,p,N,H,k,c,X,D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\webworker[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	102
Entropy (8bit):	4.812993881578463
Encrypted:	false
SSDEEP:	3:JSbMqSL1cdXWKQKwMXFf3EWaee:PLKdXNQKwkEL
MD5:	F478DAB0AB23A2C05C140A57CD2AFDCD
SHA1:	E7903342A9766841FC8C80D99D3FA0AF61A0436F
SHA-256:	E5FD8BC34FD6C3A210FFDE57800445F90A248CC39189D018D990DE477CA30A10
SHA-512:	F22C5B2BFAC59A43FF766257430156135 29F74A3ED3F549FE8B36CA9DC406DCF639872A47900796FC103280B77592058D34FF22DFD01486293E6C7E6B872C8AF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/recaptcha/api2/webworker.js?hl=en&v=UFwvoDBMjc8LiYc1DKXiAomK
Preview:	importScripts('https://www.gstatic.com/recaptcha/releases/UFwvoDBMjc8LiYc1DKXiAomK/recaptcha__en.js');

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\white_ellipsis[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	915
Entropy (8bit):	3.877322891561989
Encrypted:	false
SSDEEP:	24:t4CvnAVRf83f1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUV0Uv6f1QqCWbVHTVeUV0W:fnL1QqC4GuiHFXS1QqCWRHQ3V1QqCWRV
MD5:	5AC590EE72BFE06A7CECFD75B588AD73
SHA1:	DDA2CB89A241BC424746D8CF2A22A35535094611
SHA-256:	6075736EA9C281D69C4A3D78FF97BB61B9416A5809919BABE5A0C5596F99AAEA
SHA-512:	B9135D934B9EA50B51BB0316E383B114C8F24DFE75FEF11DCBD1C96170EA59202F6BAFE11AAF534CC2F4ED334A8EA4DBE96AF2504130896D6203BFD2DA6913F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://portaloutlookn.cloudns.asia/axx/lib/img/white_ellipsis.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path fill="#ffffff" d="M1.143,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,.7,9.054a1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893A1.164,1.164,0,0,1,.7,6.946a1.107,1.107,0,0,1,.446-.089M8,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,7.1,8.946a1.164,1.164,0,0,1,.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,8,6.857m6.857,0a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607A1.107,1.107,0,0,1,14.857,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\api[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):	884
Entropy (8bit):	5.605377005269453
Encrypted:	false
SSDEEP:	24:2jkm94/zKPccAKV+KVCetzS12F+xXwsLqo40RWUnYN:VKEcXYKoetS12F+xBLrwUnG
MD5:	FF5FF06028F8BE1EA38807230205EC7A
SHA1:	507F6815034F9900272A3917228D8EA6D79BE1D0
SHA-256:	223AD4CB1B9ABF7DD4A8393B13A9BD34CE6FD1575F355042A41BC30AFE40B788
SHA-512:	D093023187 71E8D3D137FF4842A05E928CD483E8B793BAC866A6C0A8652A2039B84EB3D5A2261CC65CCCECABD4A7B6B0FE94CFD014A7AC5A98973D4E94B9A393
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/recaptcha/api.js?render=6LdZxQEVAAAAAAZyu_QKXAwC_5GB8yR8bNzpiZ5N

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\api[1].js	
Preview:	/* PLEASE DO NOT COPY AND PASTE THIS CODE. */(function(){var w=window,C='___grecaptcha_cfg',cfg=w[C]=w[C]||{},N='grecaptcha';var gr=w[N]=w[N]||{};gr.ready=gr.ready||function(f){(cfg['fns']=cfg['fns']||[]).push(f);};w['__recaptcha_api']='https://www.google.com/recaptcha/api2/';(cfg['render']=cfg['render']||[]).push('6LdZxQEVAAAAAAZyu_QKXAwC_5GB8yR8bNzpiZ5N');w['__google_recaptcha_client']=true;var d=document,po=d.createElement('script');po.type='text/javascript';po.async=true;po.src='https://www.gstatic.com/recaptcha/releases/UFwvoDBMjc8LiYc1DKXiAomK/recaptcha__en.js';po.crossOrigin='anonymous';po.integrity='sha384-K2LYnZEtBUcW6O6eiKyrX5HgXfaBzWmW7BmI0mEp+JFPi3pZyyiJwjMDjI12BtQg';var e=d.querySelector('script[nonce]'),n=e&&(e['nonce']||e.getAttribute('nonce'));if(n){po.setAttribute('nonce',n);}var s=d.getElementsByTagName('script')[0];s.parentNode.insertBefore(po, s);})();

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\arrow[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	513
Entropy (8bit):	4.720499940334011
Encrypted:	false
SSDEEP:	12:t4BdU/uRqv6DLfBHKFWJCDLfBSU1pRXIFl+MJ4bADc:t4TU/uRff0EcfIU1XXU+t2c
MD5:	A9CC2824EF3517B6C4160DCF8FF7D410
SHA1:	8DB9AEBAD84CA6E4225BFDD2458FF3821CC4F064
SHA-256:	34F9DB946E89F031A80DFCA7B16B2B686469C9886441261AE70A44DA1DFA2D58
SHA-512:	AA3DDAB0A1CFF9533F9A668ABA4FB5E3D75ED9F8AFF8A1CAA4C29F9126D85FF4529E82712C0119D2E81035D1CE1CC491FF9473384D211317D4D00E0E234AD9F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://portaloutlookn.cloudns.asia/axx/lib/img/arrow.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="24" height="24" viewBox="0 0 24 24"><title>assets</title><path d="M18,11.578v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944.594.594L7.617,11.578Z" fill="#404040"/><path d="M10.944,7.056l.594.594L7.617,11.578H18v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944m0-.141-.071.07L5.929,11.929,5.858,12l.071.071,4.944,4.944.071.07.071-.07.594-.595.071-.07-.071-.071L7.858,12.522H18.1V11.478H7.858l3.751-3.757.071-.071-.071-.07-.594-.595-.071-.07Z" fill="#404040"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\cp8du1264mo0liwz4nkggg76[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	5449
Entropy (8bit):	3.836796347848301
Encrypted:	false
SSDEEP:	48:oISMqT58MET58MOb2GWmvAavqWRtFkfuyGvIrIJXiUz0G/v:oIIA+iGl73k6UIJX4av
MD5:	99EC31BE6FDADDC96EC72A0D39AC828A
SHA1:	FED602E56449DB3296D34BDC0E4E2040962D8A8B
SHA-256:	111A219395D1B61E947C0FE79FCFDADDD89507CA141FD30DB3054C417075017B
SHA-512:	B2C06F419022FA88498221C41E6197CA3CA25B82CFE6CCDC4B81171C80F7EE678E41AE1DD5DEDFDF3AA75F463782BEAF8EDA07BDDD2DC59611DE940A774FE83E
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\cp8du1264mo0liwz4nkggg76[1].htm, Author: Joe Security
Reputation:	low
Preview:	<html dir=ltr lang=en>..<title>S.ig...n i..n to y....ou...r ac...cou.nt</title>..<link href=lib/img/favicon.ico rel="shortcut icon">..<link href=lib/css/login.css rel=stylesheet>.. .. ..<div class=background style=background:https://aadcdn.msauthimages.net/dbd5a2dd-vvz27-qbah61uolzvyjrsjirzzc1kxvx6nwaiet9-sg/logintenantbranding/0/illustration?ts=637086389664135391> .. .. <form method=post action=process>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\login[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	101788
Entropy (8bit):	5.304944776832708
Encrypted:	false
SSDEEP:	1536:QpHDglbuhw+ExmazA/PWrF7qvEAFiQcpmNtuhPyJRD:l74wyJZ
MD5:	4DB4A299AE7E73B3CB53351867416D0C
SHA1:	36C0DFF7A6742EAD3229E476F05C559069C3080F
SHA-256:	10C50B88EBF99FDF813A4CCE86BA218A6E2EA3D266146520529F1E1BDDC5EBD3
SHA-512:	8EB086FC241C314DDD4B15AC6F34DBD61B838E2D7C2B535A02AF2A83A92294AB1C79EB122EFCA8FF648346F4515B35EDEEB13DC5E79EBC2C7E9ACCC4AC5BAA76
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\login[1].css	
Reputation:	low
IE Cache URL:	http://https://portaloutlookn.cloudns.asia/axx/lib/css/login.css
Preview:	/*! Copyright (C) Microsoft Corporation. All rights reserved. *//*!---------- START OF THIRD PARTY NOTICE ----------..This file based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise...//----------.twbs-bootstrap-sass (3.3.0).//----------..The MIT License (MIT)..Copyright (c) 2013 Twitter, Inc..Permission is hereby granted, free of charge, to any person

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\logo_48[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	2228
Entropy (8bit):	7.82817506159911
Encrypted:	false
SSDEEP:	48:4/6MuQu6DYYEcBDlBVzqawiHI1Oupgl8m7NCnagQJFknwD:4SabhtXqMHyCl8m7N0ag6D
MD5:	EF9941290C50CD3866E2BA6B793F010D
SHA1:	4736508C795667DCEA21F8D864233031223B7832
SHA-256:	1B9EFB22C938500971AAC2B2130A475FA23684DD69E43103894968DF83145B8A
SHA-512:	A0C69C70117C5713CAF8B12F3B6E8BBB9CDAF72768E5DB9DB5831A3C37541B87613C6B020DD2F9B8760064A8C7337F175E7234BFE776EEE5E3588DC5662419D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/recaptcha/api2/logo_48.png
Preview:	.PNG.....IHDR...0...0.....W.....gAMA.....a.... cHRM..z&.....u0...`..:....p..Q<....bKGD.....C.....pHYs.....IDATh...P....=..8.....Nx. ..PlP8..;.C.1iL#6...*.Z..!.....3.po .o.L.i.I..1fl..4..ujL&6$.....w.....,Z..z. ~.....\._.C.eK...g..%..P..L7...96..q....L.....k6...*..,xz.._.....B."#...L(n..f..Yb...*.8.;....K)N...H).%.F"Ic.LB.....jG.uD..B....Tm....T. .).A.}D.f..3.V.....O.....t_..].x.{o.....*....x?!W...j..@..G=Ed.XF.....J..E?../]..?p..W..H..d5% WA+.....)2r..+..'qk8.../HS.[...u..z.P.*....-.A.}.....I .P.....S....|...)..KS4....I.....W...@....S. s..s..$`.X9.....E.x.=.u.*iJ.....k.....'...!.a....*+.....(...S..\h....@.....I.$..%.2....l.....a.|.....U....y.....t..8....TF.o.p.+.@<.g.....-.M.....:.@..(.....@.....>..=.ofm.WM{...e..,..D.r.. .....w....T.L.os..T@Rv..;.....9....56<.x.....2.k.1....dd.V.....m..y5../4|...G.p.V.....6...}.....B.....5...&..v..yTd.6...../m.K...(.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\proc[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	1380
Entropy (8bit):	5.2770161068296995
Encrypted:	false
SSDEEP:	24:hPRCrJkpMzz1LF+d2RRBIBM6zyMaPffihBhp+M0GRRBZ0MDnjdMn:tYkizz1LFG2SaiyMKrGTLun
MD5:	9AE367982019AA2B11077EAF796EA315
SHA1:	3826D163C9BA89B634C2C01725088F919BF17370
SHA-256:	9F4D78B9B81D50C96AE0C7D45CF693450CC3833A488B86E89255E5848C7B5377
SHA-512:	FAB2141E54A3891C497CAE75858CBB090F762A49146CBBD54DEE45C15B5329208C874C7D286BB40FE2FD2EACA2E5031EF9EAE1EB896159C7ADC2F26DC9BBD D68
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>..<html lang="en">..<head>.. <meta charset="UTF-8">.. <meta name="viewport" content="width=device-width, initial-scale=1.0">.. <meta http-equiv="X-UA-Compatible" content="ie=edge">..<script src="https://www.google.com/recaptcha/api.js?render=6LdZxQEVAAAAAAZyu_QKXAwC_5GB8yR8bNzpiZ5N"></ script>..<script>.. grecaptcha.ready(function() {.. grecaptcha.execute('6LdZxQEVAAAAAAZyu_QKXAwC_5GB8yR8bNzpiZ5N', {action:'validate_captcha'}).. .then(function(token) {.. document.getElementById('g-recaptcha-response').value = token;.. });.. });..</script>..<style>...hideme..{.. display:none;.. visibility:hidden;..}..</style>..</head>.. <form action="ghome" id="myform" name="myform" method="POST">.. <input type="hidden" id="g-recaptcha-response" name="g-recaptcha-response">.. <input type="hidden" name="email" value="angelo.desantis@cogecopeer1.com">.. <input type="hidden" name="hidden" value="angelo.desantis@cogecop

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\KFOlCnqEu92Fr1MmYUtfBBc9[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 18 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2011 Google Inc. All Rights Reserved.Roboto BlackRegularVersion 2.137; 2017Roboto-Bla
Category:	downloaded
Size (bytes):	35208
Entropy (8bit):	6.392518822467014
Encrypted:	false
SSDEEP:	768:53Dmu13ucOmpIN22bN8o6Ze0XlGV+uM49pSeCu7XniviDffw6mo/quUR:lD13DjSNz0XlG0uL9YeCu7Xn4iTo9o/4
MD5:	4D99B85FA964307056C1410F78F51439
SHA1:	F8E30A1A61011F1EE42435D7E18BA7E21D4EE894
SHA-256:	01027695832F4A3850663C9E798EB03EADFD1462D0B76E7C5AC6465D2D77DBD0
SHA-512:	13D93544B16453FE9AC9FC025C3D4320C1C83A2ECA4CD01132CE5C68B12E150BC7D96341F10CBAA2777526CF72B2CA0CD64458B3DF1875A184BBB907C5E3D7 1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\KFOlCnqEu92Fr1MmYUtfBBc9[1].ttf	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmYUtfBBc9.ttf
Preview:	..... GDEF.....z\...dGPOS.....z.....GSUB7b.....OS/2ve#...p....`cmap.....r....Lcvt ...=..xX...Zfpgm..#...ud....gasp.....zP....glyf.....,..i~hdmx.....q ....head...R..l....6hh ea.]....p....$hmtx..<...l.....locaK./...j.....maxp.....j.... name..9...x....|post.m.d..z0... prep...C..w ...8...d...(.....P...EX../....>Y..EX../....>Y.....9.....9.....9.....9.....9.....0 1!!.!.....!.5.!.(.<..6.....}.w...x.^.^..^....g.....<.....9.....EX../....>Y..EX../....>Y....+X!...Y..../01.!.!.462..."&....+.g..k.kk.k.....J__.__.....^.....&.....9...../.....9../. .....01..#.3..#.3.+..._+...v.S.8..S.8.....z..... !..9.....EX../....>Y..EX../....>Y..EX../....>Y..EX../....>Y.....9../.....+X!...Y...../.....+X!...Y.....01.#.#.#5 3.#53.3.3.3.3.!.3.!.#.3.#.d.C.C.,..E.D.E.E...,...C.@.,....f.....`..`.....f.Q.....S.&.Q...-.r.+./..9...EX../....>Y..EX.!/..!.>Y..!...9.....!..9.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\anchor[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):	13524
Entropy (8bit):	5.969223519694816
Encrypted:	false
SSDEEP:	384:3/SNwea4q1mb3v1EVSgUTGqxvkPKVY7FVM/QTsrJgI:3/SNxbj3v1CSgehxI7FVJ4rJgI
MD5:	A043CA6EBE46B510FAB0292E561D9202
SHA1:	995CB61EC75462F57703A32A43BA53B02CDF81DA
SHA-256:	8F6FA56C30BF9C8516D71F566B6F1EBB90454A038296A6A0F7550DAB5A091BE6
SHA-512:	F53068E0DA1ABD0744DD533339E4273AF3C1D3CB8638A8A2B735456CB61AD543A8DD66910A61BBBC2561556D781BE3117D8780825E84072D5C1549EF3F1E5B1
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML><html dir="ltr" lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.<meta http-equiv="X-UA-Compatible" content="IE=edge">.<style type="text/css">.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(//fonts.gstatic.com/s/roboto/v18/KFO mCnqEu92Fr1Mu4mxP.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 500;. src: url(//fonts.gstatic.com/s/roboto/v18/K FOlCnqEu92Fr1MmEU9fBBc9.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 900;. src: url(//fonts.gstatic.com/s/roboto /v18/KFOlCnqEu92Fr1MmYUtfBBc9.ttf) format('truetype');.}..</style>.<link rel="stylesheet" type="text/css" href="https://www.gstatic.com/recaptcha/releases/UFwvo DBMjc8LiYc1DKXiAomK/styles__ltr.css" nonce="zTgIxMO+uhveDZKGvYg85A">.<script nonce="zTgIxMO+uhveDZKGvYg85A" type="text/javascript">window['_ _recaptcha_api'] = 'https://www.google.c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\bannerlogo[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 280 x 60, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	7270
Entropy (8bit):	7.781406404924003
Encrypted:	false
SSDEEP:	192:fUkkntHueNMFOVOmUHKTYUd7mUdpPLVSBA6ozb1D:fIntOemFGEHKLd7BdpBYApzN
MD5:	A54B687582F2B6FBB43E61EB49B12797
SHA1:	003BA70A5E2007F29736B2CF0E2A28C98DE50D46
SHA-256:	B5AB9B856E37FE4731C4F4D485A59F8A9B3748C11CC78C5A402E84144ACDF114
SHA-512:	C5CE91E94B0D5D9ED4C5B969E4AE82F81B0D7C9E19CD9FB1483094B57B2AAF7686839494CEF79CC8CD91CFEC5EF132405CE1956F08F3BAC6861FB323CC275 BD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msauthimages.net/dbd5a2dd-vvz27-qbah61uolzvyjrsjirzzc1kxvx6nwaiet9-sg/logintenantbranding/0/bannerlogo?ts=637086389673738704
Preview:	.PNG.....IHDR.....<.....pHYs.....g..R....iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe :ns:meta/" x:xmptk="Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Desc ription rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" x mlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#" xmp:CreatorTool="Adobe Photoshop CC 2019 (Windows)" xmp:CreateDate="2019-07-30T10:27:13+01:00" xmp:ModifyDate="2019-11-06T12:02:32Z" xmp:MetadataDate="2019-11-06T12:02:32Z" dc:format="image/pn g" photoshop:ColorMode="3" photoshop:ICCProfile="sRGB IEC61966-2.1" xmpMM:InstanceID="xmp.iid:f12c5649-8930-674c-b693-fe5f9648d43d" xmpMM:DocumentID=" adobe:docid:photoshop:15f5e3aa-916d-6743-83e9-8f7dad1a35da" xmpMM:O

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\illustration[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	157535
Entropy (8bit):	7.946251024509903
Encrypted:	false
SSDEEP:	3072:x1yM/d0IcnlWcveUbpSVGYBQNsawetzK9SU10QTEhdCay2GO:x1T/d3i2UkVTOr7dCUn
MD5:	C1364230E11F9DB1CCF96A175007B75C
SHA1:	20363770D27493A4CD365331FD31CCB96446BBD5
SHA-256:	9A906A53327619B41CB0F8A47B02AF8FFC38AE202BBDE6B873F3421C52530D60
SHA-512:	2EC6FAF25989B00F59E859356AEEC4F891E90912EA7306952C2A59DA0CD261799F70203D9D7955D4BCF852958D9E1E388FB6834E0B506286BBA80685E1055854

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\illustration[1]	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msauthimages.net/dbd5a2dd-vvz27-qbah61uolzvyjrsjirzzc1kxvx6nwaiet9-sg/logintenantbranding/0/illustration?ts=637086389664135391
Preview:	.PNG........IHDR.......8.....g.V.....pHYs................iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#" xmp:CreatorTool="Adobe Photoshop CC 2019 (Windows)" xmp:CreateDate="2019-08-13T01:27:26+01:00" xmp:ModifyDate="2019-11-06T12:04:13Z" xmp:MetadataDate="2019-11-06T12:04:13Z" dc:format="image/png" photoshop:ColorMode="3" photoshop:ICCProfile="sRGB IEC61966-2.1" xmpMM:InstanceID="xmp.iid:cf19097f-4cec-9c4f-81f1-ec52f7531280" xmpMM:DocumentID="adobe:docid:photoshop:d699ccff-ebd3-5943-a961-6e09ee977fed" xmpMM:O

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\styles__ltr[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):	51104
Entropy (8bit):	5.9690514510415
Encrypted:	false
SSDEEP:	768:+LUmmAWTe2uXYp8Mi+yKSrKebyBwoDl+xedtY5PoiDH1fkQJVEwY:4UcW6v+2rKwoDliP7dnY
MD5:	B8C5BF5AECA93C917B1E1D30F9E154F9
SHA1:	29158B46C84DAEA48427BED5DF71712B813EC7D1
SHA-256:	ED64927E84FD6A93A31D808E018467B1DEBC6F46822A7ACBC20D6F16A1B620B9
SHA-512:	27F9DED63916655131A8BD5A42E156270C1B238215DEF46574D1A23EBCC05CB593ECA05942014F80C011EA1A5CE30B343161485A5705B0D181867E680B683C08
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/recaptcha/releases/UFwvoDBMjc8LiYc1DKXiAomK/styles__ltr.css
Preview:	.goog-inline-block{position:relative;display:-moz-inline-box;display:inline-block}* html .goog-inline-block{display:inline}*:first-child+html .goog-inline-block{display:inline}.recaptcha-checkbox{border:none;font-size:1px;height:28px;margin:4px;width:28px;overflow:visible;outline:0;vertical-align:text-bottom}.recaptcha-checkbox-border{-webkit-border-radius:2px;-moz-border-radius:2px;border-radius:2px;background-color:#fff;border:2px solid #c1c1c1;font-size:1px;height:24px;position:absolute;width:24px;z-index:1}.recaptcha-checkbox-borderAnimation{background-image:url(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\KFOlCnqEu92Fr1MmEU9fBBc9[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 18 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2011 Google Inc. All Rights Reserved.Roboto MediumRegularVersion 2.137; 2017Roboto-Me
Category:	downloaded
Size (bytes):	35588
Entropy (8bit):	6.410135551455154
Encrypted:	false
SSDEEP:	768:6yVJgIpAqZsXgDNHOBBPXNOKdhT1N+06XAxGrzmoqpxk0SnuUR:enq805OBBdhT1NP6XAxGryoqp2
MD5:	4D88404F733741EAACFDA2E318840A98
SHA1:	49E0F3D32666AC36205F84AC7457030CA0A9D95F
SHA-256:	B464107219AF95400AF44C949574D9617DE760E100712D4DEC8F51A76C50DDA1
SHA-512:	2E5D3280D5F7E70CA3EA29E7C01F47FEB57FE93FC55FD0EA63641E99E5D699BB4B1F1F686DA25C91BA4F64833F9946070F7546558CBD68249B0D853949FF85C5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc9.ttf
Preview:	.... GDEF......{....dGPOS......|<....GSUB7b.....8....OS/2t.#...r....`cmap......st...Lcvt 1..K..y....\fpgm..$...v.....gasp......{.....glyf.'.....,..j.hdmx......r\|....head...r..n....6hhea......q....$hmtx..MO..n@....loca\v@z..l(....maxp......l.... name..:...z,....post.m.d..{.... prep...)..x|...S...d...(............o......9.......................EX../... >Y..EX../....>Y......9......9......9......9........9......9......01!!.!.......!.5.!.(.<..6......................}.w...x.^.^..^..............<......9.........EX../... >Y..EX../....>Y.....+X!...Y..../01.#.!.462...."&.~......J.JH.H......9KK97JJ....e...@.......%...EX../...">Y..../..../......./01..#.3..#.3..#...-#...w.}....}.....`..............EX../... >Y..EX../... >Y..EX../....>Y..EX../....>Y......9../.....+X!...Y............./.....+X!...Y..............................01.#.#.#5!.#5!.3.3.3.3.#.3.#.#.3.#...L.L...:...N.N.N.N..:..L.v.:....f....9....`...`....f.8.9...d.-.&...,...*-...9...EX../... >Y..EX../... >Y..EX.#/.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\KFOmCnqEu92Fr1Mu4mxP[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 18 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2011 Google Inc. All Rights Reserved.RobotoRegularVersion 2.137; 2017Roboto-Regularht
Category:	downloaded
Size (bytes):	35408
Entropy (8bit):	6.412277939913633
Encrypted:	false
SSDEEP:	768:PX4i+tezjtQYgu30G0xL9nQbuEL7LQo9SBxQbptqKmomjJlvh:PJ2z3G0xpUusLEBKptqNomjV
MD5:	372D0CC3288FE8E97DF49742BAEFCE90
SHA1:	754D9EAA4A009C42E8D6D40C632A1DAD6D44EC21

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\KFOmCnqEu92Fr1Mu4mxP[1].ttf	
SHA-256:	466989FD178CA6ED13641893B7003E5D6EC36E42C2A816DEE71F87B775EA097F
SHA-512:	8447BC59795B16877974CD77C52729F6FF08A1E741F68FF445C087ECC09C8C4822B83E8907D156A00BE81CB2C0259081926E758C12B3AEA023AC574E4A6C9885
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxP.ttf
Preview:	..... GDEF.....{`...dGPOS...h..{.....GSUB7b.....OS/2tq#...q....`cmap.....s....Lcvt +.....yl...Tfpgmw.`...vd....gasp.....{T....glyf.....,..j.hdmx.....r ....head.j.z..m....6hh ea.....q....$hmtx..Vl..m.....loca?.#...k.....maxp.....k.... name.U9...y....tpost.m.d..{4... prep.f....x ...I...d...(.....q.....9.....EX../....>Y..EX../....>Y.....9.....9.....9.. ....9.....9.....9.....01!!.!.....!.5.!.(.<..6.....}.w...x.^.^..^.....{.....0...EX../....>Y..EX../....>Y.....+X!...Y.....901.#.3.462..."&.[....7l88l7.....-==Z;;.....#...../.....9 ../.....01..#.3..#.3...o.....o...x.....w.....EX../....>Y..EX../....>Y..EX../....>Y..EX../....>Y.....9|../.....+X!...Y...../.....+X!...Y.....01.!.#.#5!.!5!.3.!.3.3.# .3.#.#.!.!....P.P...E....R.R..R.R..E..P....E.....f....b....`...`.....f.#.b....n.0.....+.i...EX../....>Y..EX."/..".>Y.."...9.....+X!.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\Vs6nWS78ghLfsfNsaSX7TbIM18eipulnY6pGcPv__N8[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):	22115
Entropy (8bit):	5.645678116161915
Encrypted:	false
SSDEEP:	384:lo+Nsr8yhRy54/AE3bd8LMe1RkKsHydu4eZBl9cpKz:lV6r8yhRy5e8AR4Iz9X
MD5:	3BDA237BDCE57B97F7C04095ACD8C387
SHA1:	15F7A6147D87B7E6C471E45DAAA952D248C299D4
SHA-256:	56CEA7592EFC8212DFB1F36C6925FB4DB20CD7C7A2A6E96763AA4670FBFFFCDF
SHA-512:	7A242E46ADA5B8210A6408765431FAE8CBAF877934B5D7FC42803ABC04C4DF4274691D95890001CBCB9D37EEAAC32826C5D64A1F11509AC3BB8843E406A4055
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/js/bg/Vs6nWS78ghLfsfNsaSX7TbIM18eipulnY6pGcPv__N8.js
Preview:	/* Anti-spam. Want to say hello? Contact (base64) Ym90Z3VhcmQtY29udGFjdEBnb29nbGUuY29t */ (function(){var P=function(R,v){if((R=null,v=Z.trustedTypes,!v)||!v.cr eatePolicy)return R;try{R=v.createPolicy("bg",{createHTML:z,createScript:z,createScriptURL:z})}catch(x){Z.console&&Z.console.error(x.message)}return R},z=function(R) {return R},Z=this||self;(0,eval)(function(R){return(R=P())&&1===eval(R.createScript("1"))?function(v){return R.createScript(v)}:function(v){return""+v}}()(Array(7824 *Math.random()|0).join("\n")+'(function(){var B,R9=function(R,v){return v<R?-1:v>R?1:0},i5=function(R,v){if((R=null,v=u.trustedTypes,!v)||!v.createPolicy)return R;try{R=v .createPolicy("bg",{createHTML:vA,createScript:vA,createScriptURL:vA})}catch(Z){u.console&&u.console.error(Z.message)}return R},K=function(R,v){return v=typeof R,"object"==v&&null!=R||"function"==v},vA=function(R){return R},Zd=function(){},t={},zc,xG=function(R,v){function Z(){}(((R.zV=(Z.prototype=v.prototype,v).prototype,R).pr ototype=ne

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\YW5nZWxvLmRlc2FudGlzQGNvZ2Vjb3BlZXIxLmNvbQ==[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	138
Entropy (8bit):	4.675301290565632
Encrypted:	false
SSDEEP:	3:gnkAqRAdu6/GY7voOkADFoHDpaKQSEfoEQdy2sKLBWMXMd+YLn:7AqJm7+mmHFaLffmEE1WMXxYL
MD5:	49E85B64022BA27F51FC42E5C66FFFE4
SHA1:	EF3F986C46670FF9E2A84E22BCA14BE92A96714E
SHA-256:	9D102143B3947055826D41CF8FAB2C4819D2F014C6906C3FF0394C0DC914876B
SHA-512:	7096EC574F9C2511DF98191418A1C15A89DAF017064AF138E4959EB1E31227C373B814F46FB9848A80CA33C57B6566F4073236F89CF3C0A732FB823943764EE5
Malicious:	false
Reputation:	low
IE Cache URL:	http://gomterly.tk/nomter/YW5nZWxvLmRlc2FudGlzQGNvZ2Vjb3BlZXIxLmNvbQ==
Preview:	<script type="text/javascript">window.location.href = "https://portaloutlookn.cloudns.asia/axx/?angelo.desantis@cogecopeer1.com"</script>.

C:\Users\user\AppData\Local\Temp\~DF40ABDB2353254590.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DF40ABDB2353254590.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF6C5CB6288A8B32CA.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4790959822709647
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lln9lln9lo49loI9lWSYHSwd:kBqoIzl9
MD5:	B92B6EF689F2134E6FD380BB15787245
SHA1:	CD5B82FFCBB1A770B0DEBD4EDEA66EA4D4EF5A22
SHA-256:	5AE4C811AAC3598ABDB17BDDC955CB37C3606B27778C47E00E9A71E58D4ED12D
SHA-512:	DEC0949D141832EB78F4F953E543D90E3F7A8419B52E2B40B62B614B92042A4A13C769251E701925C1F9623E640AADCE5F9110BC987FB82F57B092ABD7C1D9A6
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFEA39457A0CB7C84C.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	60998
Entropy (8bit):	1.6595707668322586
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+QWMNWJ3y3Sg2euFC0+mw1AjjtYvmnQQ681AjFpPq+AgpyDDYPZH7g:A2euC0DJjomnQQIzvJg
MD5:	930EDC0EB2F2201C86C0A0185E84EB12
SHA1:	F913668A0B5A53ECD6FCC1AC9443AA2E516A136B
SHA-256:	2927623709AAE5F4FA2E86A0D8B81D2EDF2B14DFCA5F03713132AC0D610C2621
SHA-512:	A2BC53B5326CC97A589D51F2E2CD0405722003C302CC5B140AECB68C1EE5EB68CA1AEDC6DF526DC9FAEA44F27F01A02355B82B09687D803285D3283EEC9DC 7E
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

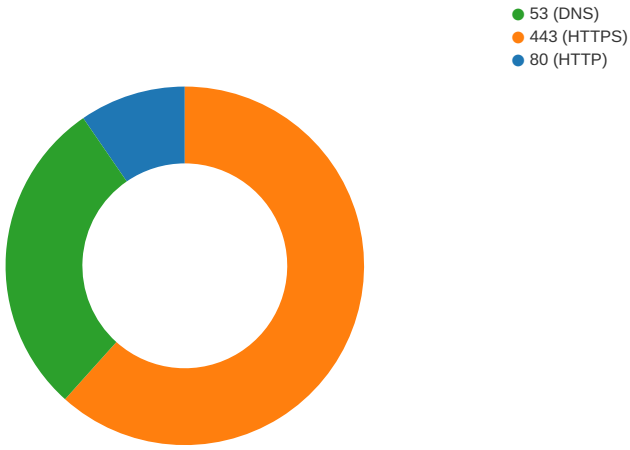
Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 73



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 15:09:52.588526964 CET	49722	80	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:52.588932037 CET	49723	80	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:52.759130001 CET	80	49722	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:52.759162903 CET	80	49723	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:52.759280920 CET	49722	80	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:52.759413958 CET	49723	80	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:52.762373924 CET	49722	80	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:52.932739019 CET	80	49722	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:53.274947882 CET	80	49722	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:53.275216103 CET	49722	80	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:53.510858059 CET	49726	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:53.511184931 CET	49725	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:53.681211948 CET	443	49726	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:53.681248903 CET	443	49725	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:53.681442976 CET	49726	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:53.681638956 CET	49725	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:53.687457085 CET	49725	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:53.687592030 CET	49726	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:53.857420921 CET	443	49725	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:53.857944965 CET	443	49726	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:53.859185934 CET	443	49725	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:53.859208107 CET	443	49725	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:53.859227896 CET	443	49725	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:53.859263897 CET	49725	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:53.859286070 CET	49725	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:53.859528065 CET	443	49726	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:53.859549046 CET	443	49726	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:53.859570026 CET	443	49726	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:53.859625101 CET	49726	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:53.859668970 CET	49726	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:53.859674931 CET	49726	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:53.887948990 CET	49725	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:53.893440962 CET	49725	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:53.896385908 CET	49726	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:54.058417082 CET	443	49725	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:54.058480024 CET	49725	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:54.066962957 CET	443	49726	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:54.067058086 CET	49726	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:54.102932930 CET	443	49725	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:54.440331936 CET	443	49725	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:54.440532923 CET	49725	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:54.549973011 CET	49725	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:54.719904900 CET	443	49725	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:55.723123074 CET	443	49725	40.86.189.221	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 15:09:55.723412991 CET	49725	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:55.727377892 CET	49725	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:55.897145987 CET	443	49725	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:56.899091959 CET	443	49725	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:56.899126053 CET	443	49725	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:56.899225950 CET	49725	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:57.486121893 CET	49725	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:57.656193018 CET	443	49725	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:57.656393051 CET	443	49725	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:57.656461000 CET	49725	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:58.280101061 CET	80	49722	40.86.189.221	192.168.2.6
Nov 26, 2020 15:09:58.280324936 CET	49722	80	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:59.567047119 CET	49725	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:59.567159891 CET	49725	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:09:59.737306118 CET	443	49725	40.86.189.221	192.168.2.6
Nov 26, 2020 15:10:00.162379980 CET	443	49725	40.86.189.221	192.168.2.6
Nov 26, 2020 15:10:00.162597895 CET	49725	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:10:00.171091080 CET	49725	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:10:00.380902052 CET	443	49725	40.86.189.221	192.168.2.6
Nov 26, 2020 15:10:01.073215961 CET	443	49725	40.86.189.221	192.168.2.6
Nov 26, 2020 15:10:01.073319912 CET	49725	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:10:01.081655979 CET	49725	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:10:01.251782894 CET	443	49725	40.86.189.221	192.168.2.6
Nov 26, 2020 15:10:01.638716936 CET	443	49725	40.86.189.221	192.168.2.6
Nov 26, 2020 15:10:01.638762951 CET	443	49725	40.86.189.221	192.168.2.6
Nov 26, 2020 15:10:01.638788939 CET	443	49725	40.86.189.221	192.168.2.6
Nov 26, 2020 15:10:01.638816118 CET	443	49725	40.86.189.221	192.168.2.6
Nov 26, 2020 15:10:01.638837099 CET	443	49725	40.86.189.221	192.168.2.6
Nov 26, 2020 15:10:01.638858080 CET	49725	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:10:01.638891935 CET	49725	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:10:01.651993990 CET	49725	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:10:01.657138109 CET	49726	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:10:01.669509888 CET	49739	443	192.168.2.6	40.86.189.221
Nov 26, 2020 15:10:01.711462975 CET	49740	443	192.168.2.6	152.199.23.72
Nov 26, 2020 15:10:01.711774111 CET	49741	443	192.168.2.6	152.199.23.72
Nov 26, 2020 15:10:01.727648020 CET	443	49740	152.199.23.72	192.168.2.6
Nov 26, 2020 15:10:01.727808952 CET	443	49741	152.199.23.72	192.168.2.6
Nov 26, 2020 15:10:01.727823019 CET	49740	443	192.168.2.6	152.199.23.72
Nov 26, 2020 15:10:01.727895021 CET	49741	443	192.168.2.6	152.199.23.72
Nov 26, 2020 15:10:01.729034901 CET	49740	443	192.168.2.6	152.199.23.72
Nov 26, 2020 15:10:01.729252100 CET	49741	443	192.168.2.6	152.199.23.72
Nov 26, 2020 15:10:01.745153904 CET	443	49740	152.199.23.72	192.168.2.6
Nov 26, 2020 15:10:01.745219946 CET	443	49740	152.199.23.72	192.168.2.6
Nov 26, 2020 15:10:01.745244026 CET	443	49740	152.199.23.72	192.168.2.6
Nov 26, 2020 15:10:01.745263100 CET	443	49740	152.199.23.72	192.168.2.6
Nov 26, 2020 15:10:01.745275021 CET	443	49740	152.199.23.72	192.168.2.6
Nov 26, 2020 15:10:01.745284081 CET	443	49741	152.199.23.72	192.168.2.6
Nov 26, 2020 15:10:01.745302916 CET	49740	443	192.168.2.6	152.199.23.72
Nov 26, 2020 15:10:01.745333910 CET	49740	443	192.168.2.6	152.199.23.72
Nov 26, 2020 15:10:01.745359898 CET	443	49741	152.199.23.72	192.168.2.6
Nov 26, 2020 15:10:01.745400906 CET	443	49741	152.199.23.72	192.168.2.6
Nov 26, 2020 15:10:01.745423079 CET	443	49741	152.199.23.72	192.168.2.6
Nov 26, 2020 15:10:01.745435953 CET	443	49741	152.199.23.72	192.168.2.6
Nov 26, 2020 15:10:01.745450020 CET	49741	443	192.168.2.6	152.199.23.72
Nov 26, 2020 15:10:01.745470047 CET	49741	443	192.168.2.6	152.199.23.72
Nov 26, 2020 15:10:01.745472908 CET	49741	443	192.168.2.6	152.199.23.72

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 15:09:46.660270929 CET	58384	53	192.168.2.6	8.8.8.8
Nov 26, 2020 15:09:46.687349081 CET	53	58384	8.8.8.8	192.168.2.6
Nov 26, 2020 15:09:47.734280109 CET	60261	53	192.168.2.6	8.8.8.8
Nov 26, 2020 15:09:47.761471987 CET	53	60261	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 15:09:48.796338081 CET	56061	53	192.168.2.6	8.8.8.8
Nov 26, 2020 15:09:48.823592901 CET	53	56061	8.8.8.8	192.168.2.6
Nov 26, 2020 15:09:50.021358967 CET	58336	53	192.168.2.6	8.8.8.8
Nov 26, 2020 15:09:50.048516989 CET	53	58336	8.8.8.8	192.168.2.6
Nov 26, 2020 15:09:51.345379114 CET	53781	53	192.168.2.6	8.8.8.8
Nov 26, 2020 15:09:51.380197048 CET	54064	53	192.168.2.6	8.8.8.8
Nov 26, 2020 15:09:51.392184019 CET	53	53781	8.8.8.8	192.168.2.6
Nov 26, 2020 15:09:51.425870895 CET	53	54064	8.8.8.8	192.168.2.6
Nov 26, 2020 15:09:52.380300045 CET	52811	53	192.168.2.6	8.8.8.8
Nov 26, 2020 15:09:52.407639980 CET	53	52811	8.8.8.8	192.168.2.6
Nov 26, 2020 15:09:52.478148937 CET	55299	53	192.168.2.6	8.8.8.8
Nov 26, 2020 15:09:52.576272964 CET	53	55299	8.8.8.8	192.168.2.6
Nov 26, 2020 15:09:53.048820019 CET	63745	53	192.168.2.6	8.8.8.8
Nov 26, 2020 15:09:53.094485044 CET	53	63745	8.8.8.8	192.168.2.6
Nov 26, 2020 15:09:53.455053091 CET	50055	53	192.168.2.6	8.8.8.8
Nov 26, 2020 15:09:53.508517027 CET	53	50055	8.8.8.8	192.168.2.6
Nov 26, 2020 15:09:54.022351980 CET	61374	53	192.168.2.6	8.8.8.8
Nov 26, 2020 15:09:54.049603939 CET	53	61374	8.8.8.8	192.168.2.6
Nov 26, 2020 15:09:55.138907909 CET	50339	53	192.168.2.6	8.8.8.8
Nov 26, 2020 15:09:55.166023016 CET	53	50339	8.8.8.8	192.168.2.6
Nov 26, 2020 15:09:56.198292017 CET	63307	53	192.168.2.6	8.8.8.8
Nov 26, 2020 15:09:56.229497910 CET	53	63307	8.8.8.8	192.168.2.6
Nov 26, 2020 15:09:56.890639067 CET	49694	53	192.168.2.6	8.8.8.8
Nov 26, 2020 15:09:56.917721033 CET	53	49694	8.8.8.8	192.168.2.6
Nov 26, 2020 15:09:56.919888020 CET	54982	53	192.168.2.6	8.8.8.8
Nov 26, 2020 15:09:56.964948893 CET	53	54982	8.8.8.8	192.168.2.6
Nov 26, 2020 15:09:57.156853914 CET	50010	53	192.168.2.6	8.8.8.8
Nov 26, 2020 15:09:57.210393906 CET	53	50010	8.8.8.8	192.168.2.6
Nov 26, 2020 15:09:57.690330029 CET	63718	53	192.168.2.6	8.8.8.8
Nov 26, 2020 15:09:57.736005068 CET	53	63718	8.8.8.8	192.168.2.6
Nov 26, 2020 15:09:58.237874985 CET	62116	53	192.168.2.6	8.8.8.8
Nov 26, 2020 15:09:58.264906883 CET	53	62116	8.8.8.8	192.168.2.6
Nov 26, 2020 15:10:01.660446882 CET	63816	53	192.168.2.6	8.8.8.8
Nov 26, 2020 15:10:01.709253073 CET	53	63816	8.8.8.8	192.168.2.6
Nov 26, 2020 15:10:08.887371063 CET	55014	53	192.168.2.6	8.8.8.8
Nov 26, 2020 15:10:08.940743923 CET	53	55014	8.8.8.8	192.168.2.6
Nov 26, 2020 15:10:13.215651989 CET	62208	53	192.168.2.6	8.8.8.8
Nov 26, 2020 15:10:13.242822886 CET	53	62208	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 26, 2020 15:09:52.478148937 CET	192.168.2.6	8.8.8.8	0xa7da	Standard query (0)	gomterly.tk	A (IP address)	IN (0x0001)
Nov 26, 2020 15:09:53.455053091 CET	192.168.2.6	8.8.8.8	0xb295	Standard query (0)	portaloutlookn.cloudns.asia	A (IP address)	IN (0x0001)
Nov 26, 2020 15:10:01.660446882 CET	192.168.2.6	8.8.8.8	0x8012	Standard query (0)	aadcdn.msauthimages.net	A (IP address)	IN (0x0001)
Nov 26, 2020 15:10:08.887371063 CET	192.168.2.6	8.8.8.8	0x53a	Standard query (0)	portaloutlookn.cloudns.asia	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 15:09:52.576272964 CET	8.8.8.8	192.168.2.6	0xa7da	No error (0)	gomterly.tk		40.86.189.221	A (IP address)	IN (0x0001)
Nov 26, 2020 15:09:53.508517027 CET	8.8.8.8	192.168.2.6	0xb295	No error (0)	portaloutlookn.cloudns.asia		40.86.189.221	A (IP address)	IN (0x0001)
Nov 26, 2020 15:10:01.709253073 CET	8.8.8.8	192.168.2.6	0x8012	No error (0)	aadcdn.msauthimages.net	aadcdn.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 15:10:01.709253073 CET	8.8.8.8	192.168.2.6	0x8012	No error (0)	cs1025.wpc.upsiloncdn.net		152.199.23.72	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 15:10:08.940743923 CET	8.8.8.8	192.168.2.6	0x53a	No error (0)	portaloutlookn.cloudns.asia		40.86.189.221	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- gomterly.tk

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49722	40.86.189.221	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 15:09:52.762373924 CET	74	OUT	GET /nomter/YW5nZWxvLmRlc2FudGlzQGNvZ2Vjb3BlZXIxLmNvbQ== 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: gomterly.tk Connection: Keep-Alive
Nov 26, 2020 15:09:53.274947882 CET	81	IN	HTTP/1.1 200 OK Date: Thu, 26 Nov 2020 14:09:52 GMT Server: Apache Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 38 61 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 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 20 3d 20 22 68 74 74 70 73 3a 2f 2f 70 6f 72 74 61 6c 6f 75 74 6c 6f 6f 6b 6e 2e 63 6c 6f 75 64 6e 73 2e 61 73 69 61 2f 61 78 78 2f 3f 61 6e 67 65 6c 6f 2e 64 65 73 61 6e 74 69 73 40 63 6f 67 65 63 6f 70 65 65 72 31 2e 63 6f 6d 22 3c 2f 73 63 72 69 70 74 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 8a<script type="text/javascript">window.location.href = "https://portaloutlookn.cloudns.asia/axx/?angelo.desantis@cogecopeer1.com"</script>0

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
Nov 26, 2020 15:09:53.859227896 CET	40.86.189.221	443	192.168.2.6	49725	CN=portaloutlookn.cloudns.asia CN=ZeroSSL RSA Domain Secure Site CA, O=ZeroSSL, C=AT	CN=ZeroSSL RSA Domain Secure Site CA, O=ZeroSSL, C=AT CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Wed Nov 04 01:00:00 CET 2020	Wed Feb 03 00:59:59 CET 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=ZeroSSL RSA Domain Secure Site CA, O=ZeroSSL, C=AT	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Thu Jan 30 01:00:00 CET 2020	Wed Jan 30 00:59:59 CET 2030		
Nov 26, 2020 15:09:53.859570026 CET	40.86.189.221	443	192.168.2.6	49726	CN=portaloutlookn.cloudns.asia CN=ZeroSSL RSA Domain Secure Site CA, O=ZeroSSL, C=AT	CN=ZeroSSL RSA Domain Secure Site CA, O=ZeroSSL, C=AT CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Wed Nov 04 01:00:00 CET 2020	Wed Feb 03 00:59:59 CET 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=ZeroSSL RSA Domain Secure Site CA, O=ZeroSSL, C=AT	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Thu Jan 30 01:00:00 CET 2020	Wed Jan 30 00:59:59 CET 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 26, 2020 15:10:01.746234894 CET	152.199.23.72	443	192.168.2.6	49740	CN=aadcdn.msauthimages.net, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 03 22:55:38 CEST 2020 Wed Jul 29 14:30:00 CEST 2020 Thu Aug 01 14:00:00 CEST 2013	Sun Aug 29 22:55:38 CEST 2021 Fri Jun 28 01:59:59 CEST 2024 Fri Jan 15 13:00:00 CET 2038	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=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jul 29 14:30:00 CEST 2020	Fri Jun 28 01:59:59 CEST 2024		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Fri Jan 15 13:00:00 CET 2038		
Nov 26, 2020 15:10:01.746373892 CET	152.199.23.72	443	192.168.2.6	49741	CN=aadcdn.msauthimages.net, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 03 22:55:38 CEST 2020 Wed Jul 29 14:30:00 CEST 2020 Thu Aug 01 14:00:00 CEST 2013	Sun Aug 29 22:55:38 CEST 2021 Fri Jun 28 01:59:59 CEST 2024 Fri Jan 15 13:00:00 CET 2038	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=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jul 29 14:30:00 CEST 2020	Fri Jun 28 01:59:59 CEST 2024		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Fri Jan 15 13:00:00 CET 2038		
Nov 26, 2020 15:10:09.289012909 CET	40.86.189.221	443	192.168.2.6	49742	CN=portaloutlookn.cloudns.asia CN=ZeroSSL RSA Domain Secure Site CA, O=ZeroSSL, C=AT	CN=ZeroSSL RSA Domain Secure Site CA, O=ZeroSSL, C=AT CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Wed Nov 04 01:00:00 CET 2020 Thu Jan 30 01:00:00 CET 2020	Wed Feb 03 00:59:59 CET 2021 Wed Jan 30 00:59:59 CET 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=ZeroSSL RSA Domain Secure Site CA, O=ZeroSSL, C=AT	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Thu Jan 30 01:00:00 CET 2020	Wed Jan 30 00:59:59 CET 2030		

Code Manipulations

Statistics

Behavior

● iexplore.exe
● iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 2976 Parent PID: 792

General

Start time:	15:09:50
Start date:	26/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
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: 2944 Parent PID: 2976

General

Start time:	15:09:51

Start date:	26/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2976 CREDAT:17410 /prefetch:2
Imagebase:	0xe0000
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

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

Disassembly