ID: 323467
Cookbook: browseurl.jbs
Time: 02:39:56
Date: 27/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

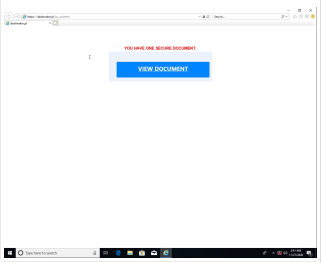
Analysis Report https://dealmaker.pl/au_au.html

Overview

General Information

Sample URL:	http://https://dealmaker.pl/au_au.html
Analysis ID:	323467

Most interesting Screenshot:



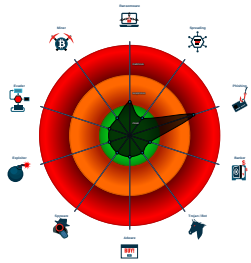
Detection

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

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected HtmlPhish_30
- HTML body contains low number of …
- HTML title does not match URL
- Suspicious form URL found

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6904 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6948 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6904 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

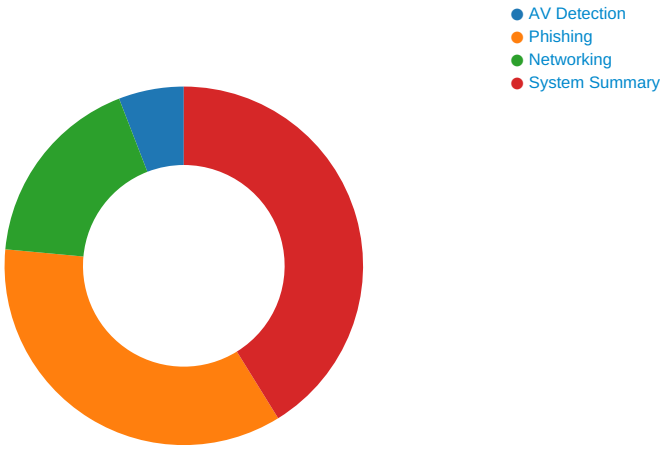
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\au_au[1].htm	JoeSecurity_HtmlPhish_30	Yara detected HtmlPhish_30	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

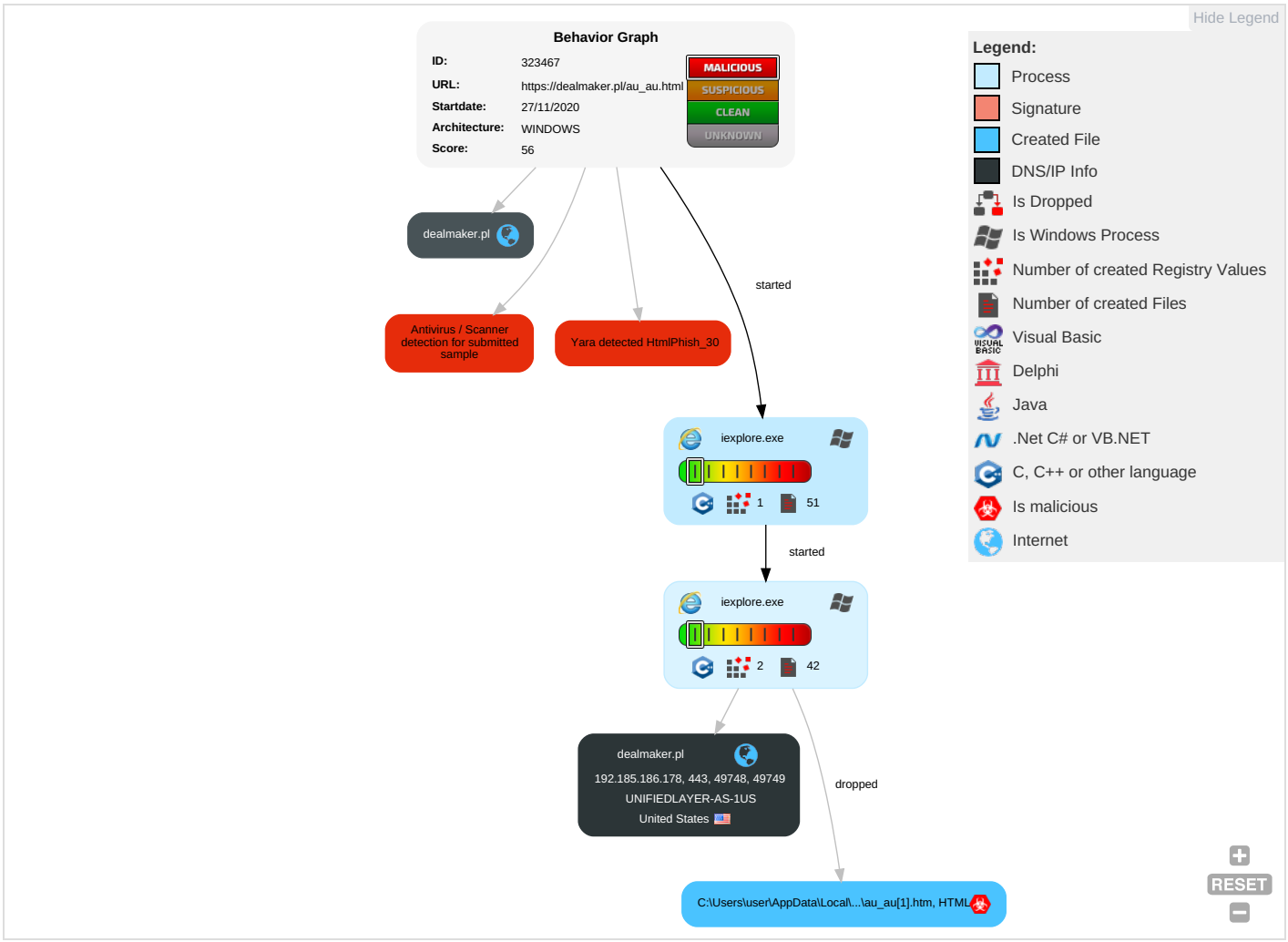
Phishing:

Yara detected HtmlPhish_30

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	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lockc
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data

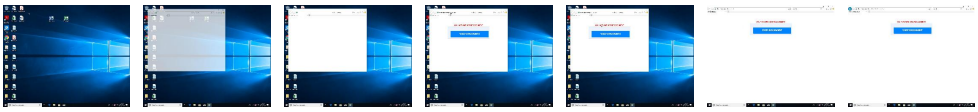
Behavior Graph

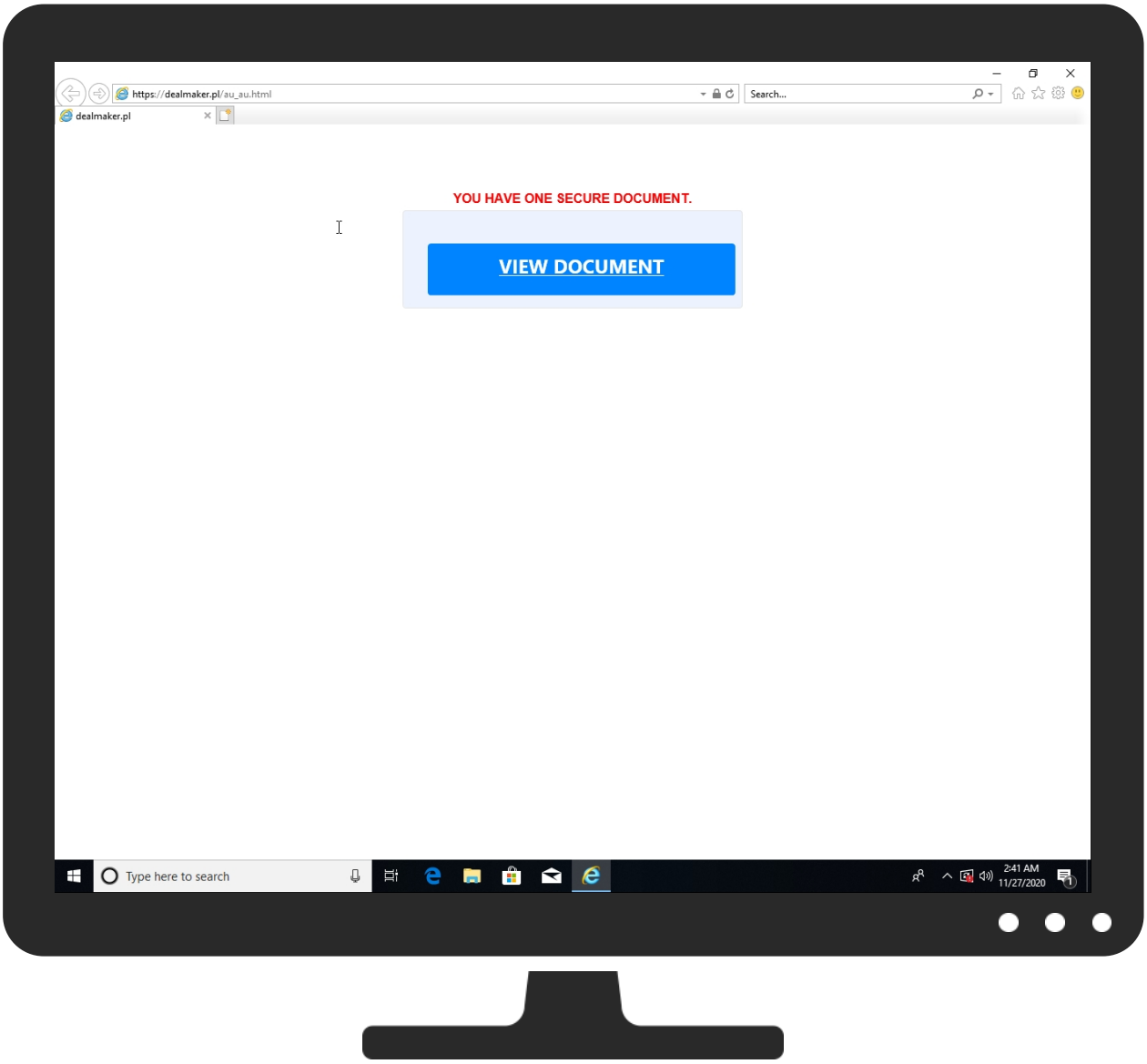


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://dealmaker.pl/au_au.html	0%	Virustotal		Browse
http://https://dealmaker.pl/au_au.html	0%	Avira URL Cloud	safe	
http://https://dealmaker.pl/au_au.html	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://www.onlineaspect.com)	0%	Avira URL Cloud	safe	
http://https://dealmaker.pl/P	0%	Avira URL Cloud	safe	
http://https://dealmaker.pl/Pu_au.html	0%	Avira URL Cloud	safe	
http://https://www.google.%/ads/ga-audiences?	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences?	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences?	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences?	0%	URL Reputation	safe	
http://https://silversky.com/privacy-policy/	0%	Avira URL Cloud	safe	
http://www.silversky.com/	0%	Avira URL Cloud	safe	
http://https://dealmaker.pl/au_au.htmlRoot	0%	Avira URL Cloud	safe	
http://https://dealmaker.pl/PDF_NEW_AU/PDF_NEW_AU	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dealmaker.pl	192.185.186.178	true	false		unknown

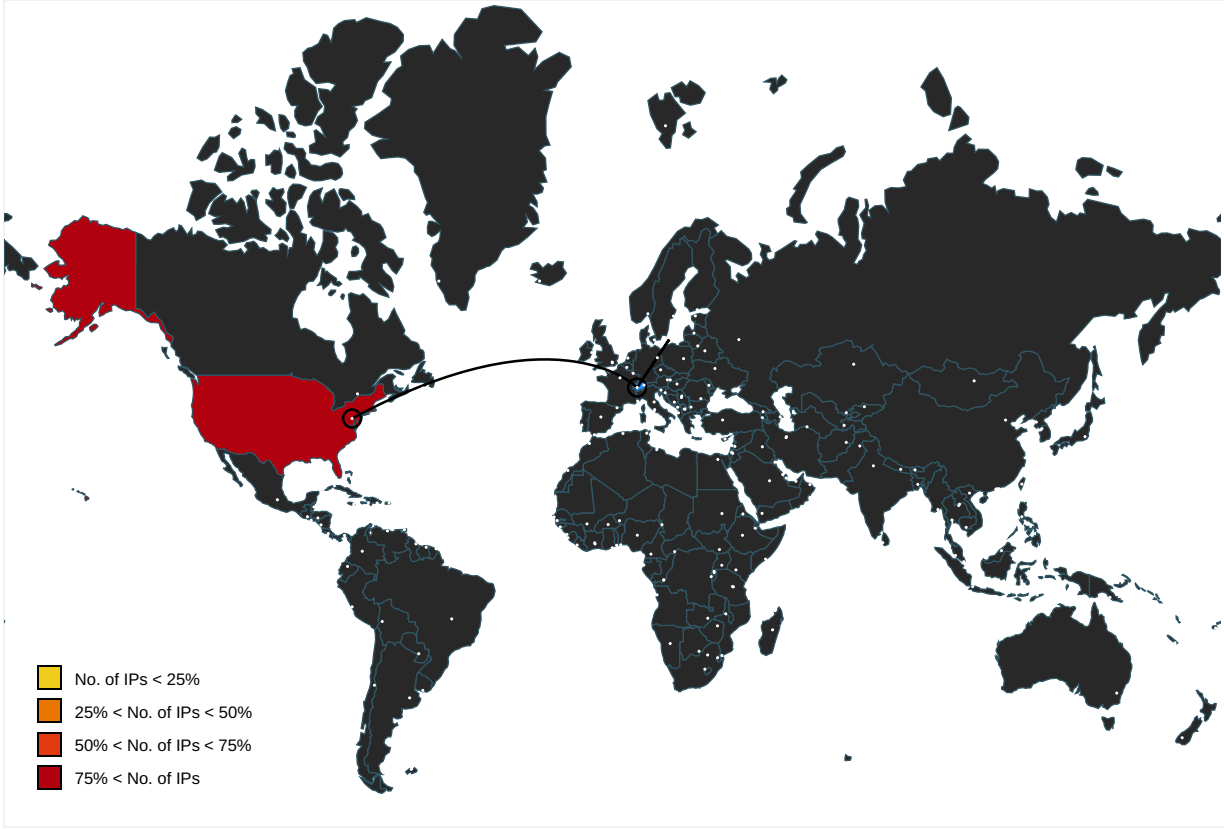
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://dealmaker.pl/PDF_NEW_AU/PDF_NEW_AU/	true		unknown
http://https://dealmaker.pl/au_au.html	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.onlineaspect.com)	detect_timezone[1].js.2.dr	false	• Avira URL Cloud: safe	low
http://https://dealmaker.pl/P	{90926100-3051-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://dealmaker.pl/Pu_au.html	{90926100-3051-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.google.%/ads/ga-audiences?	ga[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://stats.g.doubleclick.net/j/collect?	ga[1].js.2.dr	false		high
http://https://silversky.com/privacy-policy/	PDF_NEW_AU[1].htm0.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.silversky.com/	PDF_NEW_AU[1].htm0.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://dealmaker.pl/au_au.html	{90926100-3051-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true		unknown
http://https://dealmaker.pl/PDF_NEW_AU/PDF_NEW_AU/	~DFFCCD4F00A28E9D19.TMP.1.dr, PDF_NEW_AU[1].htm.2.dr	false		unknown
http://https://dealmaker.pl/au_au.htmlRoot	{90926100-3051-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://dealmaker.pl/PDF_NEW_AU/PDF_NEW_AU	au_au[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://mailsafe.perimeterusa.com/tpl/Door/Login	PDF_NEW_AU[1].htm0.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.186.178	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323467
Start date:	27.11.2020
Start time:	02:39:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://dealmaker.pl/au_au.html
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:	8
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.phis.win@3/13@2/1
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://dealmaker.pl/PDF_NEW_AU/PDF_NEW_AU

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.147.198.201, 40.88.32.150, 104.83.120.32, 51.104.144.132, 172.217.168.72, 172.217.168.68, 52.155.217.156 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, displaycatalog.md.mp.microsoft.com.akadns.net, arc.msn.com, skypedataprdcoleus16.cloudapp.net, e11290.dspg.akamaiedge.net, ssl.google-analytics.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, ssl-google-analytics.l.google.com, www.google.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{909260FE-3051-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{909260FE-3051-11EB-90EB-ECF4BBEA1588}.dat	
Entropy (8bit):	1.8401986032788213
Encrypted:	false
SSDEEP:	192:rCZhZw/2wao9Wwa8otwa8tHifwa8tsIcezMwa8Ahsj2Bwa8AbsTQDwa8AbXsusf2:r+nfGUvBNvVK2
MD5:	04526DF515BE8E6C4CBDF5A7665E1F4D
SHA1:	CD57121ACA460A49CBDC9BD9FADCCB5813E5491E
SHA-256:	3B084F490D66836EA8C8F2EAD492A0C004A90E292E4ABA1E0F16D550873542CE
SHA-512:	EB12412A78E683398793FA365A3790E67CEE82E9CAA9D05B20D1DFD4E790E4D9BE4DFB70C9D90565756220315232 3C894E85B90027C25E6169FA188B91158B68
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\{90926100-3051-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	34076
Entropy (8bit):	1.8695772135120934
Encrypted:	false
SSDEEP:	192:rKZ9Q96PkKcFj52gkWYMrYwLjbviPCEpRc2:r2CoMKchIk9rBXb66kL
MD5:	D682F73A8172B00C5230A13908FDED73
SHA1:	06D8B093B0893B2E8446C623B8108F2AE2C8DAEE
SHA-256:	089D0A54BD2753EA5CAEF6521FDF51E1AB908FC0589B6AFBBDE89326347DDA23
SHA-512:	3F7532524F0E10C323367A719AAD193F42AE833D440FA1F2481EA614D55F863BF85BF08DA311D9CA280F36A07F790BD448DC272EA653DF8CF17B5A5B05C811E1
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\{90926101-3051-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5655385809370568
Encrypted:	false
SSDEEP:	48:IwbGcprqGwpaRG4pQJGrapbScrGQpKCG7HpR+sTGIpG:rBZyQD6pBScFAtT+4A
MD5:	A050F12338E538E38A89D515B56E2253
SHA1:	466EE08FB22BDBD76CA033BB4BD26BE2F911F71F
SHA-256:	2035E7023E536B980A5ED12F3932A824076BA097D6D6D3AF4F749E0011DA942E
SHA-512:	FFB84F4FBCD737AD7EAF12B8D9F6E9190C958133D9BB62C8941C6C2F6ED5333CC5375A762BDC7A895E4BAC596D884CD51E3281B297030600CCA4A79DB0FA4E E9
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\au_au[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	3460
Entropy (8bit):	5.788717534543746
Encrypted:	false
SSDEEP:	96:ym8ZKOMrm2zHldVpA0AMddddddddddddddddddddddddddddddddddBmfJO5g9i3:yJZKDrm2zHtESEi3
MD5:	7408EC5E1B8EB5C9B4CB1C4E6094B12F
SHA1:	ACF261BCA64030443DE98F89C364DFFEB685727F
SHA-256:	170CD17E7A2B9E1A9FE992B712828229E150E45205DC704F1F366491774B8C9C
SHA-512:	8C9B5649AD7B2CC4C34E9822A3E4F0C425882E42D032B41379C3B3385B19F2D44A840240E17DECB3A2EC6FFACF9DA2DF551B0F9B47F475E60EF326739537857

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\au_au[1].htm	
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_30, Description: Yara detected HtmlPhish_30, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\au_au[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://dealmaker.pl/au_au.html
Preview:	<HTML><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/></head><BODY><P> </P>..<TABLE id=gmail-m_44728256438462 0020email_table style="MAX-WIDTH: 420px; HEIGHT: 202px; WIDTH: 574px; BORDER-COLLAPSE: collapse; MARGIN: 0px auto" cellSpacing=0 cellPadding=0 align=c enter border=0>..<TBODY>..<TR>..<TD id=gmail-m_44728256438462 0020email_content style='FONT-FAMILY: "Helvetica Neue", Helvetica, "Lucida Grande", tahoma, verdana, arial, sans-serif; BACKGROUND: rgb(255,255,255)'>..<P align=center> </P>..<TABLE style="BORDER-COLLAPSE: collapse" cellSpacing=0 cell Padding=0 width="100%" border=0>..<TBODY>..<TR>..<TD>..<TABLE style="BORDER-COLLAPSE: collapse" cellSpacing=0 cellPadding=0 width="100%" border=0>..<T BODY>..<TR>..<TD style="LINE-HEIGHT: 28px" height=28>..<P align=center><STRONG><FONT color=#ff0000>YOU HAVE ONE SECURE DOCUMENT.</FONT> </STRONG></P></TD></TR>..<TR>..<TD>..<TABLE style="BORDER-COLLAPSE: collapse" cellSpacing=0 cellPadding=0 width="100%" border

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\commoncombined[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	exported SGML document, ASCII text, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	53301
Entropy (8bit):	5.246286546938678
Encrypted:	false
SSDEEP:	768:4D+qqNZYcHuY9qh8HNqX7td6NxHDuv34vCow:G+FNmcHuY9tHNqD2xHDII7w
MD5:	4D3FF67AA0D5A92F67B6BB38CD88A993
SHA1:	F579D37E1F9A1F5E5D62E7A54E5A93C54CCB5802
SHA-256:	E3B8A436585D41F5BEDAE298C15C52004847CF59B2262601C8C0341CECCF7519
SHA-512:	7C9A7152CFD971285457D7A5862259D6ACAE2B9966A59481718B9098C618CF61229266D252A5DC23AF62A79BDE15DBB37BE4777E5D21557C6D81550526714743
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dealmaker.pl/PDF_NEW_AU/PDF_NEW_AU/commoncombined.js
Preview:	@(#) USA.NET mailsafetpl C8.MAIN.4.26B 11:05:19:15:19:09 -->./**..* @constructor..*/....DHTML_modalMessage = function()..{...var htmlOfModalMessage = '';...// html of modal message...var isvisible = false;...../var divs_modalDiv;.../var divs_modalBgDiv;.../var divs_modalCardDiv;.../var divs_modalCardHeader;.../var divs_ modalCardBody;.../var divs_modalCardFooter;.....var divs_modalMsg;...var divs_modalMsgContent;...var divs_modalMsgContentBox;...var divs_modalMsgCloseButton ;..}....DHTML_modalMessage.prototype = {.../ {{{ setHtmlContent(newHtmlContent).. /**.. *.Setting static HTML content for the modal dialog box... * ... *. @param String newHtmlContent = Static HTML content of box.. *.. * @public... */.....setHtmlContent : function(newHtmlContent)...{....this.htmlOfModalMessage = newHtmlContent;.....}..../ }}}...../ {{{ setSize(width,height).. /**.. *.Set the size of the modal dialog box.. * ... *.@param int width = width

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\detect_timezone[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	exported SGML document, ASCII text, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	15244
Entropy (8bit):	5.114740372039098
Encrypted:	false
SSDEEP:	192:2W2IamGMJGi/SX6rChmB8DoDmV9DLsVHcpxaYFkmytFjFst8UbRXX3U:ZazYGcCpHsVHpYDCt36E
MD5:	33AECB8F705606C482DE0167759160F6
SHA1:	05B2FAE279E3696282A274798F675E17FA602D8E
SHA-256:	DB2624E55A11A1024F9FAF673F31E24BE74BB1AC3BF8836D1E7F8BAA80C80FAA
SHA-512:	3202ACBC5B85517BBAF6BEEEDF382D073FA5894EF955094272AF02BC6D28EA827AB2CEC0889C4182232ED05C530310034ED0E89620BC735E17C81F0DBAE05B E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dealmaker.pl/PDF_NEW_AU/PDF_NEW_AU/detect_timezone.js
Preview:	@(#) USA.NET mailsafetpl C8.MAIN.4.26B 11:05:19:15:19:05 -->./* .. * Original script by Josh Fraser (http://www.onlineaspect.com).. * Continued by Jon Nylander, (jon at pageloom dot com).. * According to both of us, you are absolutely free to do whatever .. * you want with this code... * .. * This code is maintained at bitbucket.org as jsTimezoneDetect... */..../**.. * Namespace to hold all the code for timezone detection... */..var jzTimezoneDetector = new Object();....jzTimezoneDetector.HEMISPHERE_S OUTH = 'SOUTH';..jzTimezoneDetector.HEMISPHERE_NORTH = 'NORTH';..jzTimezoneDetector.HEMISPHERE_UNKNOWN = 'N/A';..jzTimezoneDetector.olson = {};..../**.. * A simple object containing information of utc_offset, which olson timezone key to use, .. * and if the timezone cares about daylight savings or not... * .. * @constr uctor.. * @param {string} offset - for example '-11:00'.. * @param {string} olson_tz - the olson Identifier, such as "America/Denver".. * @param {boolean} uses_dst - fl

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\main.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	285929
Entropy (8bit):	5.032454971439158
Encrypted:	false
SSDEEP:	1536:mXOvNqIURcTPUC4/vMHBBC8gd7nsDSrqUpv:GOwROPj4/vYBCVdjGLYv
MD5:	AD323561D984A7583FA9A5D39A324D21

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\main.min[1].css	
SHA1:	7B215C8BD11BF74D2B7B8344DB652CEC83488334
SHA-256:	66F08AB2F619FC9BDE59EE2F9CF9FF368728618D13335EADE73411DA05CD6CD2
SHA-512:	6ECD8F7D062C44D32B96D341474B600BCBBE3FDD2FFCA2342C5F48DDA547A8C98E4327913FB58ABA52FC2E89F619CAE4C15F3FF4CB8C1AB125C6888B12A67 19
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dealmaker.pl/PDF_NEW_AU/PDF_NEW_AU/main.min.css
Preview:	/* @(#) USA.NET mailsafetpl C8.MAIN.4.26B 11:05:19:15:19:03 main.min.css@@/main/15 */./*! email-encryption v2.0.0 | (c) 2019 Doug Follette | proprietary License */.@keyframes a{0%{transform:rotate(0deg)}to{transform:rotate(359deg)}}.breadcrumb,.button,.delete,.file,.is-unselectable,.modal-close,.pagination-ellipsis,.pagination-l ink,.pagination-next,.pagination-previous,.tabs{-webkit-touch-callout:none;-webkit-user-select:none;-moz-user-select:none;-ms-user-select:none;user-select:none}.navbar- link:not(.is-arrowless):after,.select:not(.is-multiple):not(.is-loading):after{border:3px solid transparent;border-radius:2px;border-right:0;border-top:0;content:" ";displa y:block;height:.625em;margin-top:-.4375em;pointer-events:none;position:absolute;top:50%;transform:rotate(-45deg);transform-origin:center;width:.625em}.block:not(:last- child),.box:not(:last-child),.breadcrumb:not(:last-child),.content:not(:last-child),.highlight:not(:last-child),.level:not(:last-child),.list:not(:last-child),.mes

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\PDF_NEW_AU[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	251
Entropy (8bit):	5.198033800059641
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwol6hEr6VX16hu9nPLNso3w+KqD:J0+ox0RJWWPLNFT
MD5:	51BA6000408B3741823D713662844F31
SHA1:	997CC028B6D6750135B005159B01A0910450411D
SHA-256:	46C591E91FCF126171D7F88C2325108CF231A8BFF50256C77B48F0845C7A0CEF
SHA-512:	6ABF8BB9739C58164DEFAB12A8453F4B6D9D0109B919AD19BA099A90D1F30296939490F47C42AA7918887745DF1679C1F9B4FAA5956529ECD3B5265D84E36353
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>301 Moved Permanently</title>.</head><body>. Moved Permanently . The document has moved here. .</body></html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\PDF_NEW_AU[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	3307
Entropy (8bit):	5.344806308811007
Encrypted:	false
SSDEEP:	96:QOrNQfDu7Bf+D4JtC0Fi29kJHlxLIzZs71:QOBQLuNmDatlFOhTLIzg1
MD5:	831934274457BD206918B4334D9AF376
SHA1:	897F8583AAC1F649251597010C493C417859B5B6
SHA-256:	4E958CB13C1734F9010B5E006AE0CE5B26CE873FEEFCC550A2316F75485593C9
SHA-512:	A95923E2288CCFF6EFAF1E4A2C0E89EA07F74AA4E02DB06DCA1A293960C253864572033C35E7CA35549BC63D6A5CC4A91D14BC2A7D233C2ACC3F172A7A44A1 10
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dealmaker.pl/PDF_NEW_AU/PDF_NEW_AU/
Preview:	..<!DOCTYPE html>.. (generation C8.MAIN.4.25Zmsweb01.mailsafe.usa.net) (C) USA.NET, Inc. -->....<html>..<head>...<meta charset="utf-8">.. <meta http-equ iv="X-UA-Compatible" content="IE=edge">.. <meta name="viewport" content="width=device-width, initial-scale=1">...<title>Email Encryption</title>...<link href ="main.min.css" rel="stylesheet" type="text/css">...<link rel="icon" type="image/png" sizes="192x192" href="https://www.google.com/s2/favicons?domain=?v=BUILD_H ASH" id="favimg">..<style type="text/css">.. ..#navbar {.. border-bottom: 2px solid #A3A5AB;..}....-->..</style>....<script type="text/javascript">....var _gaq = _gaq || [];.._ gaq.push(['_setAccount', 'UA-24146012-5']);.._gaq.push(['_trackPageview']);....(function() {...var ga = document.createElement('script'); ga.type = 'text/javascript'; ga.async = true;...ga.src = ('https:' == document.location.protocol ? 'https://ssl' : 'http://www') + '.google-analytics.com/ga.js';...var s = document.getElementsByTagN

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\ga[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	46274
Entropy (8bit):	5.48786904450865
Encrypted:	false
SSDEEP:	768:aqNVrKn0VGhn+K7U1r2p/Y60fyy3/g3OMZht1z1prkfw1+9NZ5VA:RHrLVGhnpIwp/Y7cnz1RkLL5m
MD5:	E9372F0EBBCF71F851E3D321EF2A8E5A
SHA1:	2C7D19D1AF7D97085C977D1B69DCB8B84483D87C
SHA-256:	1259EA99BD76596239BFD3102C679EB0A5052578DC526B0452F4D42F8BCDD45F
SHA-512:	C3A1C74AC968FC2FA366D9C25442162773DB9AF1289ADFB165FC71E7750A7E62BD22F424F241730F3C2427AFFF8A540C214B3B97219A360A231D4875E6DDEE6

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\ga[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.google-analytics.com/ga.js

Preview:

```
(function(){var E;var g=window,n=document,p=function(a){var b=g._gaUserPrefs;if(b&&b.ioo&&b.ioo()||a&&!0===g["ga-disable-"+a])return!0;try{var c=g.external;if(c
&&c._gaUserPrefs&&"oo"==c._gaUserPrefs)return!0}catch(f){}a=[];b=n.cookie.split(";");c=/^\s*AMP_TOKEN=\s*(.*?)\s*$/;for(var d=0;d<b.length;d++){var e=b[d].match
(c);e&&a.push(e[1])}for(b=0;b<a.length;b++)if("$OPT_OUT"==decodeURIComponent(a[b]))return!0;return!1};var q=function(a){return encodeURIComponent?enco
deURIComponent(a).replace(/\(/g,"%28").replace(/\)/g,"%29"):a},r=/^(www\.)?google(\.com?)?(\.[a-z]{2})?$/,u=/(^|\.)doubleclick\.net$/i;function Aa(a,b){switch(b){case 0:r
eturn""+a;case 1:return 1*a;case 2:return!!a;case 3:return 1E3*a}return a}function Ba(a){return"function"==typeof a}function Ca(a){return void 0!=a&&-1<(a.constructor+"")
.indexOf("String")}function F(a,b){return void 0==a||"-"==a&&!b||""==a}function Da(a){if(!a||""==a)return"";for(;a&&-1<" \n\r\t".indexOf(a.charAt(0));)a=a.substring(1);for(;a&&-
1<" \n\r\t".i
```

C:\Users\user\AppData\Local\Temp\~DFC47929C17D3041B0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.467031255874561
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lowS9lowC9lWwQvqXtsqXAJXAb1ts1t3:kBqoIwdwbwaqXtsqXAJXAb1ts1t3
MD5:	C4F157AC294DC1BD8665662415177D58
SHA1:	7D75D3206553400EEBCD3475AFE35F156F9B2F1A
SHA-256:	8F7E38EB0A6A0596AD0F5373239D350CE80D7123DBFE37EA10F3F49D91D4EA84
SHA-512:	684B28380662DBD85DE65750361A0C85F884EB8611CACA7E067BC25861B57E6EDC352CFC2BCF88C5A762BCB94607081C9C23ACCBF3AECCBD0F7BF1AC25B67 7D
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFCF8F74BB9AB4BD78.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
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFFCCD4F00A28E9D19.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	43593
Entropy (8bit):	0.45883123183806057
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+1bZIkIkkqWuWwl8FWwGAjO0yqWmqazbDqLz:kBqoxKAuvScS+1bZILXLdyaDn4
MD5:	8A4695999F7743BCA273D50DA16B6B8A
SHA1:	E5532FAE339054510CDCDE978A2325E7C46D4A66
SHA-256:	676D66D8B18E18B97B3BDFB91106AB4505E038FDDCBCBC46B2F6F252CD4737B2
SHA-512:	24EC95B913DC4A7C107BCF565211B4DBF90E15C07167095DF15F4E4354979CF95A08E54C4CAFFC29FD5B097C989CAE0B53D3124546C954097093A095A4360FF/
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DFFCCD4F00A28E9D19.TMP	
Preview:	..............................*%..H..M..{y..+.0...(.................... ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 02:40:46.297481060 CET	49748	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:46.301732063 CET	49749	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:46.445763111 CET	443	49749	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:46.445807934 CET	443	49748	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:46.445954084 CET	49749	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:46.446161032 CET	49748	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:46.458372116 CET	49749	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:46.458785057 CET	49748	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:46.594633102 CET	443	49749	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:46.594676018 CET	443	49748	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:46.696285009 CET	443	49749	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:46.696340084 CET	443	49749	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:46.696371078 CET	443	49749	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:46.696435928 CET	49749	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:46.696482897 CET	49749	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:46.696619034 CET	443	49748	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:46.696669102 CET	443	49748	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:46.696702957 CET	443	49748	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:46.696739912 CET	49748	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:46.696831942 CET	49748	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:46.735768080 CET	49748	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:46.736254930 CET	49749	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:46.742898941 CET	49749	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:46.743048906 CET	49748	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:46.743205070 CET	49749	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:46.874162912 CET	443	49748	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:46.874205112 CET	443	49749	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:46.884980917 CET	443	49749	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:46.885025024 CET	443	49748	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:46.885072947 CET	49749	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:46.885086060 CET	49748	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:46.905446053 CET	443	49749	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:46.905493975 CET	443	49749	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:46.905527115 CET	443	49748	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:46.905605078 CET	49748	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:46.905621052 CET	49749	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:46.905844927 CET	49748	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:46.905940056 CET	49749	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:47.080739021 CET	443	49749	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:47.080791950 CET	443	49748	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:48.010190964 CET	443	49749	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:48.010234118 CET	443	49749	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:48.010454893 CET	49749	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:48.498758078 CET	49749	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:48.646049023 CET	443	49749	192.185.186.178	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 02:40:48.757055044 CET	443	49749	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:48.757246971 CET	49749	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:53.736795902 CET	443	49749	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:53.736973047 CET	49749	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:53.744915962 CET	443	49749	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:53.744940042 CET	443	49749	192.185.186.178	192.168.2.4
Nov 27, 2020 02:40:53.745111942 CET	49749	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:53.745157003 CET	49749	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:53.746319056 CET	49749	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:40:53.881748915 CET	443	49749	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:02.516887903 CET	49752	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:41:02.651106119 CET	443	49752	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:02.651195049 CET	49752	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:41:02.653258085 CET	49752	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:41:02.803924084 CET	443	49752	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:02.938009977 CET	443	49752	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:02.938097954 CET	443	49752	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:02.938098907 CET	49752	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:41:02.938132048 CET	443	49752	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:02.938160896 CET	49752	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:41:02.938177109 CET	49752	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:41:02.943794966 CET	49752	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:41:03.103933096 CET	443	49752	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:03.118825912 CET	443	49752	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:03.118999958 CET	49752	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:41:03.146167040 CET	49752	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:41:03.320878029 CET	443	49752	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:03.635590076 CET	443	49752	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:03.636042118 CET	49752	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:41:04.271583080 CET	49748	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:41:04.412929058 CET	443	49748	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:04.696538925 CET	443	49748	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:04.696676970 CET	49748	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:41:04.700145960 CET	49748	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:41:04.834327936 CET	443	49748	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:04.915292978 CET	443	49748	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:04.915420055 CET	443	49748	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:04.915452957 CET	49748	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:41:04.915488958 CET	49748	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:41:04.921865940 CET	49748	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:41:04.922307968 CET	49748	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:41:04.922792912 CET	49748	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:41:05.055917025 CET	443	49748	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:05.056374073 CET	443	49748	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:05.056746006 CET	443	49748	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:05.231563091 CET	443	49748	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:05.231749058 CET	49748	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:41:05.235307932 CET	443	49748	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:05.235337019 CET	443	49748	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:05.235349894 CET	443	49748	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:05.235420942 CET	443	49748	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:05.235443115 CET	443	49748	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:05.235445023 CET	49748	443	192.168.2.4	192.185.186.178
Nov 27, 2020 02:41:05.235460997 CET	443	49748	192.185.186.178	192.168.2.4
Nov 27, 2020 02:41:05.235481024 CET	443	49748	192.185.186.178	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 02:40:39.989790916 CET	56534	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:40:40.017046928 CET	53	56534	8.8.8.8	192.168.2.4
Nov 27, 2020 02:40:40.696012974 CET	56627	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:40:40.741944075 CET	53	56627	8.8.8.8	192.168.2.4
Nov 27, 2020 02:40:41.386018038 CET	56621	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 02:40:41.431425095 CET	53	56621	8.8.8.8	192.168.2.4
Nov 27, 2020 02:40:42.610857964 CET	63116	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:40:42.656519890 CET	53	63116	8.8.8.8	192.168.2.4
Nov 27, 2020 02:40:43.506506920 CET	64078	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:40:43.552519083 CET	53	64078	8.8.8.8	192.168.2.4
Nov 27, 2020 02:40:44.410630941 CET	64801	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:40:44.456032991 CET	53	64801	8.8.8.8	192.168.2.4
Nov 27, 2020 02:40:45.099513054 CET	61721	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:40:45.146908045 CET	53	61721	8.8.8.8	192.168.2.4
Nov 27, 2020 02:40:46.095807076 CET	51255	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:40:46.113831997 CET	61522	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:40:46.159024000 CET	53	61522	8.8.8.8	192.168.2.4
Nov 27, 2020 02:40:46.284187078 CET	53	51255	8.8.8.8	192.168.2.4
Nov 27, 2020 02:40:47.464850903 CET	52337	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:40:47.492034912 CET	53	52337	8.8.8.8	192.168.2.4
Nov 27, 2020 02:40:48.671513081 CET	55046	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:40:48.698971033 CET	53	55046	8.8.8.8	192.168.2.4
Nov 27, 2020 02:41:02.469032049 CET	49612	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:41:02.514678001 CET	53	49612	8.8.8.8	192.168.2.4
Nov 27, 2020 02:41:04.539500952 CET	49285	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:41:04.566782951 CET	53	49285	8.8.8.8	192.168.2.4
Nov 27, 2020 02:41:05.570414066 CET	50601	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:41:05.623756886 CET	53	50601	8.8.8.8	192.168.2.4
Nov 27, 2020 02:41:05.857706070 CET	60875	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:41:05.884985924 CET	53	60875	8.8.8.8	192.168.2.4
Nov 27, 2020 02:41:13.721446037 CET	56448	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:41:13.767302036 CET	53	56448	8.8.8.8	192.168.2.4
Nov 27, 2020 02:41:14.219446898 CET	59172	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:41:14.265160084 CET	53	59172	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 02:40:46.095807076 CET	192.168.2.4	8.8.8.8	0xdb60	Standard query (0)	dealmaker.pl	A (IP address)	IN (0x0001)
Nov 27, 2020 02:41:02.469032049 CET	192.168.2.4	8.8.8.8	0xcfff	Standard query (0)	dealmaker.pl	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 02:40:46.284187078 CET	8.8.8.8	192.168.2.4	0xdb60	No error (0)	dealmaker.pl		192.185.186.178	A (IP address)	IN (0x0001)
Nov 27, 2020 02:41:02.514678001 CET	8.8.8.8	192.168.2.4	0xcfff	No error (0)	dealmaker.pl		192.185.186.178	A (IP address)	IN (0x0001)

HTTPS Packets

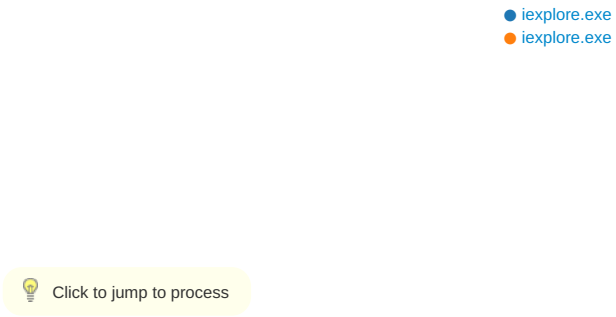
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 27, 2020 02:40:46.696371078 CET	192.185.186.178	443	192.168.2.4	49749	CN=cpcontacts.dealmaker.pl CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 16:36:19 CEST 2020	Tue Jan 05 15:36:19 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=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 27, 2020 02:40:46.696702957 CET	192.185.186.178	443	192.168.2.4	49748	CN=cpcontacts.dealmaker.pl CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 16:36:19 CEST 2020 Thu Mar 17 17:40:46 CET 2016	Tue Jan 05 15:36:19 CET 2021 Wed Mar 17 17:40:46 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=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Nov 27, 2020 02:41:02.938132048 CET	192.185.186.178	443	192.168.2.4	49752	CN=cpcontacts.dealmaker.pl CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 16:36:19 CEST 2020 Thu Mar 17 17:40:46 CET 2016	Tue Jan 05 15:36:19 CET 2021 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 6904 Parent PID: 800

General

Start time:	02:40:44
Start date:	27/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff775360000
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: 6948 Parent PID: 6904

General

Start time:	02:40:45
Start date:	27/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6904 CREDAT:17410 /prefetch:2
Imagebase:	0xd20000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly