ID: 323493
Cookbook: browseurl.jbs
Time: 03:26:18
Date: 27/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

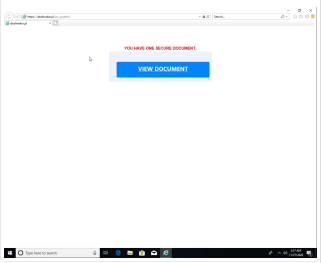
Analysis Report https://dealmaker.pl/au_au.html

Overview

General Information

Sample URL:	http://https://dealmaker.pl/au_au.html
Analysis ID:	323493

Most interesting Screenshot:



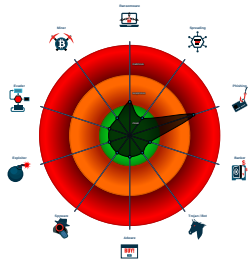
Detection

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- 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: 6776 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6828 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6776 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

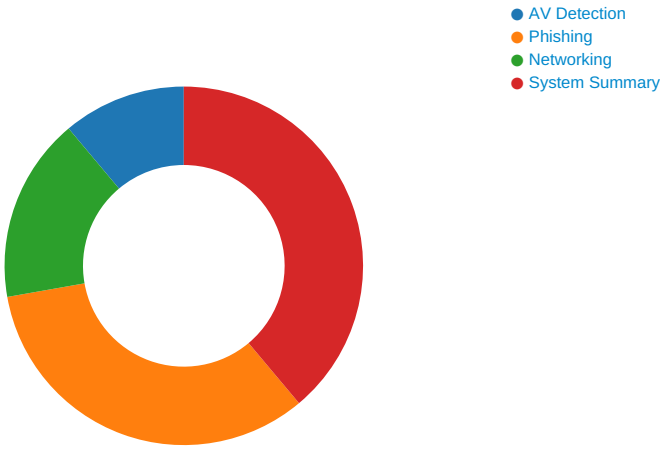
Dropped Files

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

Antivirus detection for URL or domain

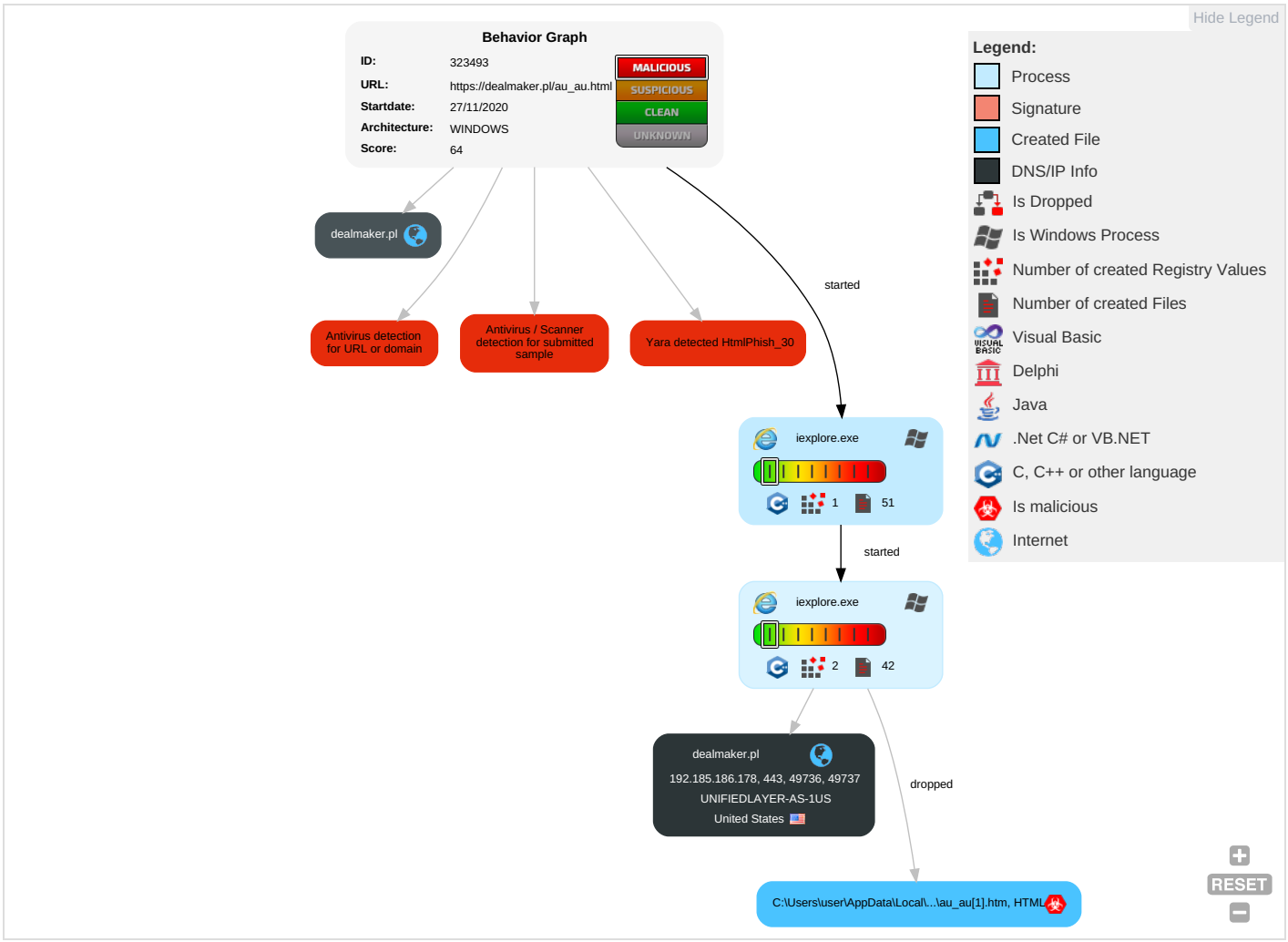
Phishing:

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

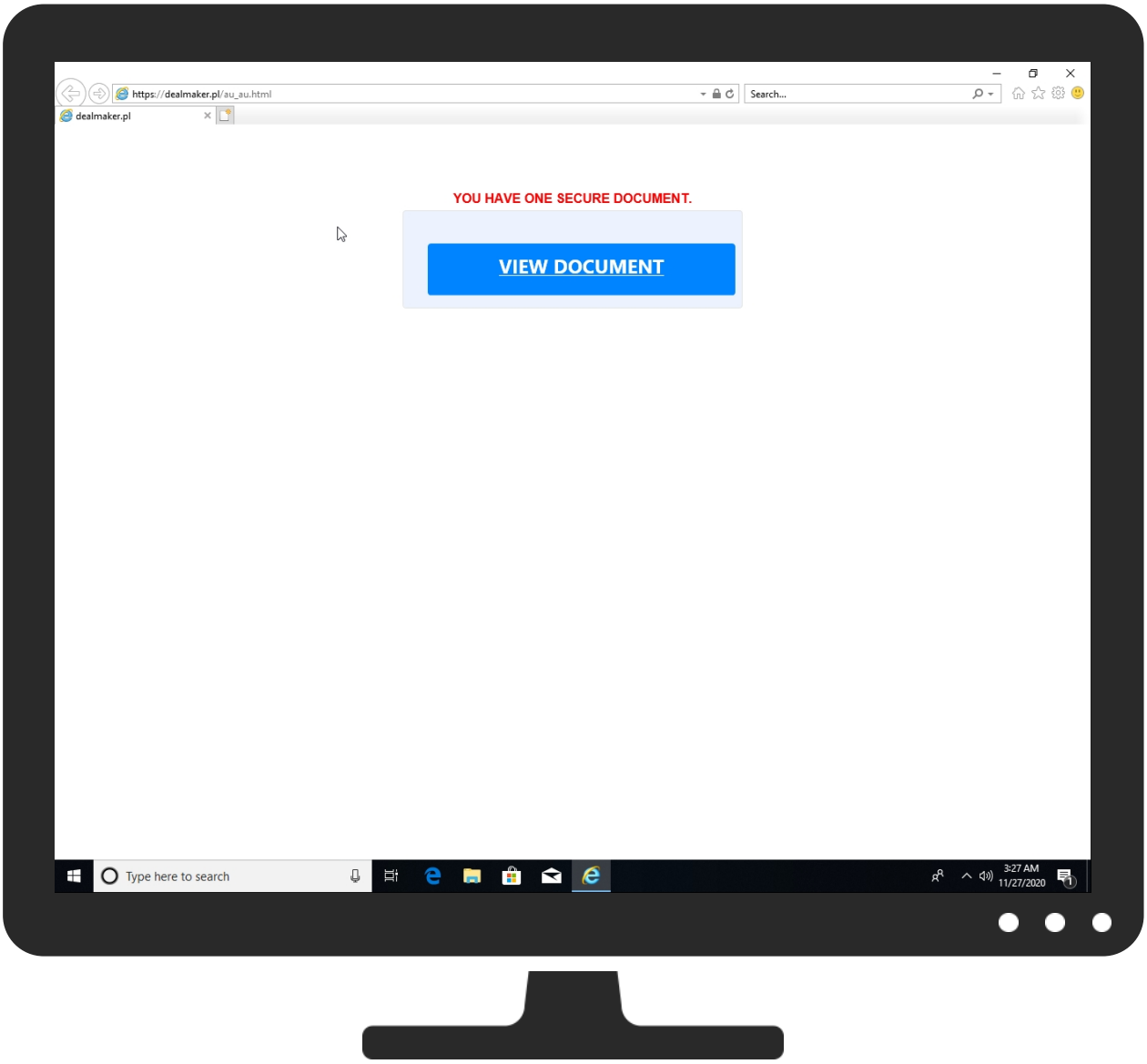
Behavior Graph



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://https://dealmaker.pl/PDF_NEW_AU/PDF_NEW_AU/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
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://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

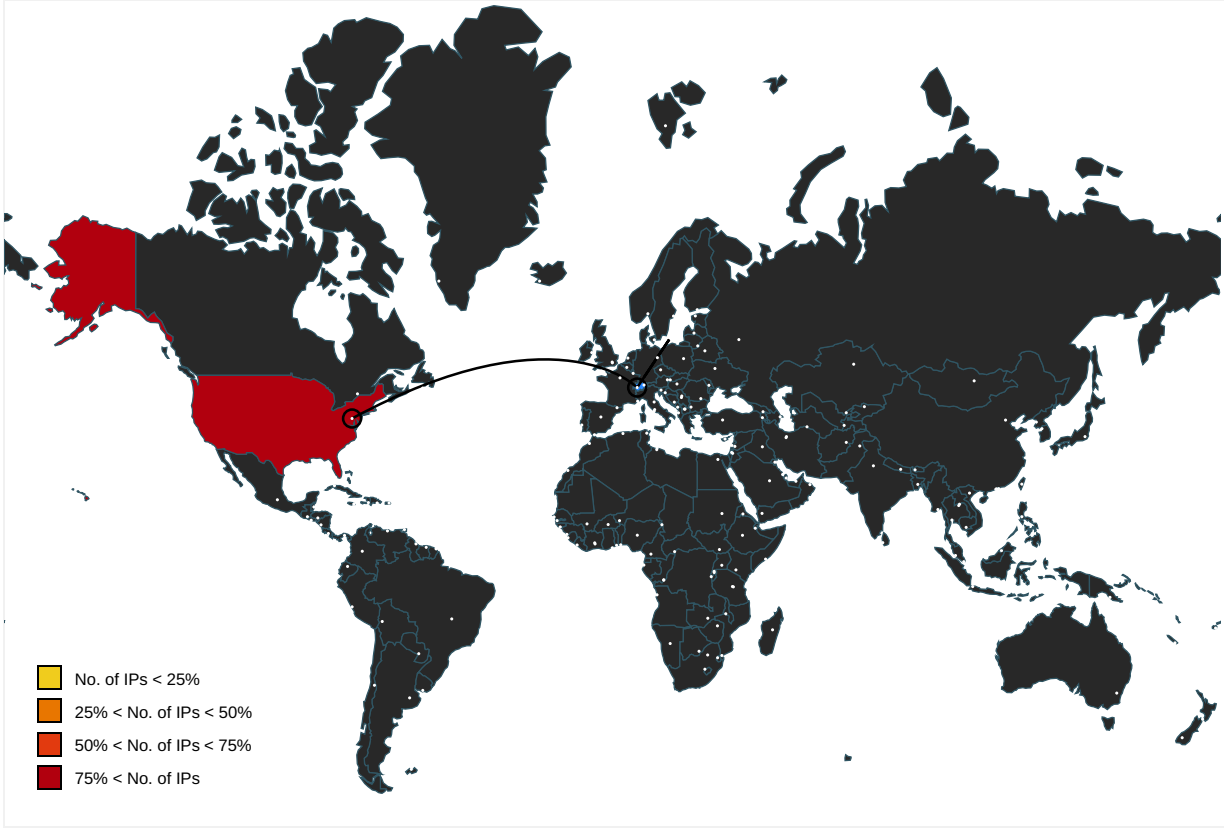
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://dealmaker.pl/PDF_NEW_AU/PDF_NEW_AU/	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	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	{0B1B1BCE-3058-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://dealmaker.pl/Pu_au.html	{0B1B1BCE-3058-11EB-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	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	{0B1B1BCE-3058-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true		unknown
http://https://dealmaker.pl/PDF_NEW_AU/PDF_NEW_AU/	~DFA23A7C22E4CF062F.TMP.1.dr, PDF_NEW_AU[1].htm.2.dr	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://dealmaker.pl/au_au.htmlRoot	{0B1B1BCE-3058-11EB-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:	323493
Start date:	27.11.2020
Start time:	03:26:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 59s
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:	7
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@3/13@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 • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.83.120.32, 51.104.139.180, 172.217.168.72, 172.217.168.68, 40.88.32.150, 104.43.193.48, 152.199.19.161, 104.42.151.234, 52.155.217.156 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, ie9comview.vo.msecnd.net, displaycatalog.md.mp.microsoft.com.akadns.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, e11290.dspg.akamaiedge.net, ssl.google-analytics.com, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, go.microsoft.com.edgekey.net, blobcollector.events.data.trafficmanager.net, ssl-google-analytics.l.google.com, www.google.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net

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.{0B1B1BCC-3058-11EB-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.{0B1B1BCC-3058-11EB-90EB-ECF4BBEA1588}.dat	
Entropy (8bit):	1.8474573050695493
Encrypted:	false
SSDEEP:	192:rjZhZS72SM09WSMOntSMOp0ifSMOpvsbVzMSMOLVvBtBSMOLVvLnDSMOLVIvisfD:rlnF+UAG+O0LD
MD5:	D88C813D51B1C236876F8B2ED65A7586
SHA1:	50F25203C1B30F50DAACB24488FDFB0B034E3C86
SHA-256:	4A5F6C2E998A8C0DC14F5D4790F72361976343382A76A4FF7EB7E8BD88CCDF2E
SHA-512:	A1D77E98DF6CEE2E1825F88A53EF69057D75D774C68FDA5E53548172E985F68973CB450FA78279C7F6E52BB868F325BD00F7691969BEDF195F6CA7CBBD83F63
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\{0B1B1BCE-3058-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	37802
Entropy (8bit):	1.9482051307259916
Encrypted:	false
SSDEEP:	192:raZtQt6vkPFjx2UkWJM8YwUj2DirC5pyco9AZBEs:rGyYsPhgAS8BW2+2/09AZN
MD5:	02A26DB1FFC0C5A3A92E42364FD87227
SHA1:	275333BC85CACB9506B1A0F44C17C6706C80CA10
SHA-256:	D6EE31F75E33EF9CEE9487DAA679855AC28A64814C507E3A4A9B4B7A94748EBE
SHA-512:	8FE8E5110091D1C03E6A1D6DAEE19FB86B22C694F7981A81CC47036CFEF81F9619E9E3869803B1972775DA3EA4361E58DBD7209ABCB2EBB15435F5AD631A142A
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\{0B1B1BCF-3058-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.565919491434874
Encrypted:	false
SSDEEP:	48:Iw90GcprLfGwpaV0G4pQfmGrapbSfrGQpKtG7HpR+sTGIpG:raZFQO6gBSfFAMT+4A
MD5:	46781FDCE8B5718BCE3E326B77C3BE6E
SHA1:	B072C1FE3440DA947CC2D1FC0066C1AC1741D720
SHA-256:	5B85CF4A86A92D2C4D86D7D922CCFDCBE24A514E21FCA19671532C02398A7427
SHA-512:	121C9463A57347A1485621DEF6B04627B4F328266FE92A3102B72F89F2819FAF5DA88926022D3D8705D0C9C1D04D1C5130C164A03C04D83D4C4F0CC50C6CA023
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\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\PDF_NEW_AU[1].htm	
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\9026IKNJ\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
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\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\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
SHA1:	7B215C8BD11BF74D2B7B8344DB652CEC83488334
SHA-256:	66F08AB2F619FC9BDE59EE2F9CF9FF368728618D13335EADE73411DA05CD6CD2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\main.min[1].css	
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\Temp\~DF69A64691B97DA382.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\~DF6C4DF8067ED1362D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47098897314828464
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loSS9loSC9lWSMupvuLILVlvI3:kBqoISdSbSMupvuLILVlvI3
MD5:	062A97615909ED625C8814C60033A439
SHA1:	AE549F31AE33C1EFA2B0DCA03BAB800A0AA4EAEF
SHA-256:	973544C644157497A1516DC5F8D2D8FCBF9ACA6576BE7ED77E049097871341BA
SHA-512:	21406750A95191179AFC79126059F01CDF303BB6C134CB32836DB7D03DD8B307BC9925C2973534F7C5783BA37826BFB8587A435FDA38FBDA91F9429103CE9846
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFA23A7C22E4CF062F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	44631
Entropy (8bit):	0.5695170482001468
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+mg6TgMWd4xOnZej9twi/+u0:kBqoxKAuqR+mg6TgMWWxos9
MD5:	84547C9041B07EF1EEC7B2DC73FEEFB6
SHA1:	251887D2BAEFCAA8357511E02F7BE0B55172E3BF
SHA-256:	9A9517B2A282AAB0CF22C9BA158EC9576B922A4A0B9D757524F1124402609F09
SHA-512:	2B7953C384A638DAAA28A5DC736CD99FAEA96E582DED7DF9901A49CBBE8FFADA071C52F68F25356F80DDAF03FA02AD39AC3C566769721CD82182C58D91AD7 90
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DFA23A7C22E4CF062F.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 03:27:09.161578894 CET	49737	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:09.161830902 CET	49736	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:09.311817884 CET	443	49736	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:09.311847925 CET	443	49737	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:09.312028885 CET	49736	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:09.312078953 CET	49737	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:09.328946114 CET	49736	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:09.328995943 CET	49737	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:09.475498915 CET	443	49736	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:09.475528002 CET	443	49737	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:09.475541115 CET	443	49736	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:09.475553036 CET	443	49736	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:09.475563049 CET	443	49736	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:09.475579977 CET	443	49737	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:09.475593090 CET	443	49737	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:09.475601912 CET	443	49737	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:09.475795031 CET	49736	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:09.475843906 CET	49737	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:09.514472961 CET	49737	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:09.515721083 CET	49736	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:09.520478964 CET	49737	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:09.520582914 CET	49736	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:09.520611048 CET	49737	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:09.663146973 CET	443	49737	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:09.663203955 CET	443	49737	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:09.663290977 CET	49737	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:09.663347006 CET	49737	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:09.665050030 CET	49737	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:09.670748949 CET	443	49736	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:09.670790911 CET	443	49736	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:09.670816898 CET	443	49736	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:09.670845032 CET	443	49737	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:09.670870066 CET	443	49737	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:09.670977116 CET	49736	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:09.671040058 CET	49737	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:09.672105074 CET	49736	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:09.774173975 CET	443	49737	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:09.774197102 CET	443	49737	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:09.774358034 CET	49737	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:09.853969097 CET	443	49737	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:09.864779949 CET	443	49736	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:09.990755081 CET	49737	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:10.131088972 CET	443	49737	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:10.256326914 CET	443	49737	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:10.256493092 CET	49737	443	192.168.2.4	192.185.186.178

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 03:27:16.262916088 CET	443	49737	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:16.262939930 CET	443	49737	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:16.262953997 CET	443	49737	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:16.262979031 CET	49737	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:16.263008118 CET	49737	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:16.263024092 CET	49737	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:16.265317917 CET	49737	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:16.399972916 CET	443	49737	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:25.290378094 CET	49738	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:25.434762955 CET	443	49738	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:25.434954882 CET	49738	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:25.440121889 CET	49738	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:25.587546110 CET	443	49738	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:25.587569952 CET	443	49738	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:25.587584972 CET	443	49738	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:25.587598085 CET	443	49738	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:25.587646008 CET	49738	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:25.587682009 CET	49738	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:25.593950033 CET	49738	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:25.746660948 CET	443	49738	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:25.746778011 CET	49738	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:25.749331951 CET	49738	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:25.951783895 CET	443	49738	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:26.031773090 CET	443	49738	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:26.033205032 CET	49738	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:27.062164068 CET	49736	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:27.216548920 CET	443	49736	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:27.545145035 CET	443	49736	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:27.545346022 CET	49736	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:27.548202038 CET	49736	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:27.702785969 CET	443	49736	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:27.802232981 CET	443	49736	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:27.802313089 CET	443	49736	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:27.802424908 CET	49736	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:27.805083990 CET	49736	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:27.811244965 CET	49736	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:27.812596083 CET	49736	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:27.812736034 CET	49736	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:27.946484089 CET	443	49736	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:27.960830927 CET	443	49736	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:27.960882902 CET	443	49736	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:28.074016094 CET	443	49736	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:28.074068069 CET	443	49736	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:28.074157953 CET	443	49736	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:28.074197054 CET	443	49736	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:28.074229002 CET	49736	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:28.074235916 CET	443	49736	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:28.074270964 CET	49736	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:28.074276924 CET	443	49736	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:28.074279070 CET	49736	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:28.074284077 CET	49736	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:28.074289083 CET	49736	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:28.074323893 CET	443	49736	192.185.186.178	192.168.2.4
Nov 27, 2020 03:27:28.074331999 CET	49736	443	192.168.2.4	192.185.186.178
Nov 27, 2020 03:27:28.074383974 CET	49736	443	192.168.2.4	192.185.186.178

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 03:27:08.022789955 CET	63153	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:08.070226908 CET	53	63153	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:08.954768896 CET	52991	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:09.144721031 CET	53	52991	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:25.242494106 CET	53700	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 03:27:25.288053036 CET	53	53700	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:26.755135059 CET	51726	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:26.782139063 CET	53	51726	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:28.456535101 CET	56794	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:28.483691931 CET	53	56794	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:28.901052952 CET	56534	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:28.946496964 CET	53	56534	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:31.628010988 CET	56627	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:31.673209906 CET	53	56627	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:32.268232107 CET	56621	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:32.295737982 CET	53	56621	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:33.066360950 CET	63116	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:33.093750954 CET	53	63116	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:33.861581087 CET	64078	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:33.888762951 CET	53	64078	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:35.003951073 CET	64801	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:35.049351931 CET	53	64801	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:35.675580978 CET	61721	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:35.720962048 CET	53	61721	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:36.496723890 CET	51255	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:36.542023897 CET	53	51255	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:37.341433048 CET	61522	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:37.368639946 CET	53	61522	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:37.996010065 CET	52337	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:38.023312092 CET	53	52337	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:38.129851103 CET	55046	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:38.175390959 CET	53	55046	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:38.620585918 CET	49612	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:38.666646004 CET	53	49612	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:39.007108927 CET	52337	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:39.052337885 CET	53	52337	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:39.254693985 CET	49285	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:39.334548950 CET	53	49285	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:39.630790949 CET	49612	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:39.638237000 CET	50601	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:39.658082008 CET	53	49612	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:39.726301908 CET	53	50601	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:39.878484011 CET	60875	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:39.923666000 CET	53	60875	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:40.021984100 CET	52337	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:40.031174898 CET	56448	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:40.049138069 CET	53	52337	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:40.076415062 CET	53	56448	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:40.647231102 CET	49612	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:40.694384098 CET	53	49612	8.8.8.8	192.168.2.4
Nov 27, 2020 03:27:41.205084085 CET	59172	53	192.168.2.4	8.8.8.8
Nov 27, 2020 03:27:41.250991106 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 03:27:08.954768896 CET	192.168.2.4	8.8.8.8	0x4b85	Standard query (0)	dealmaker.pl	A (IP address)	IN (0x0001)
Nov 27, 2020 03:27:25.242494106 CET	192.168.2.4	8.8.8.8	0x7927	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 03:27:09.144721031 CET	8.8.8.8	192.168.2.4	0x4b85	No error (0)	dealmaker.pl		192.185.186.178	A (IP address)	IN (0x0001)
Nov 27, 2020 03:27:25.288053036 CET	8.8.8.8	192.168.2.4	0x7927	No error (0)	dealmaker.pl		192.185.186.178	A (IP address)	IN (0x0001)

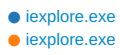
HTTPS Packets

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 03:27:09.475563049 CET	192.185.186.178	443	192.168.2.4	49736	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		
Nov 27, 2020 03:27:09.475601912 CET	192.185.186.178	443	192.168.2.4	49737	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		
Nov 27, 2020 03:27:25.587598085 CET	192.185.186.178	443	192.168.2.4	49738	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	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



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6776 Parent PID: 800

General

Start time:	03:27:07
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:	0x7ff645be0000
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: 6828 Parent PID: 6776

General

Start time:	03:27:07
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:6776 CREDAT:17410 /prefetch:2
Imagebase:	0xeb0000
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