ID: 412661
Cookbook: browseurl.jbs
Time: 20:54:27
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

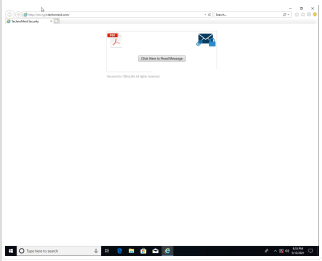
Analysis Report http://encrypt.techomind.com

Overview

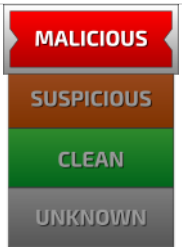
General Information

Sample URL:	http://encrypt.techomind.com
Analysis ID:	412661
Infos:	

Most interesting Screenshot:



Detection



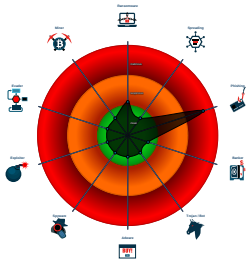
HTMLPhisher

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Phishing site detected (based on sh…
- Yara detected HtmlPhish10
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 3236 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5364 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3236 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

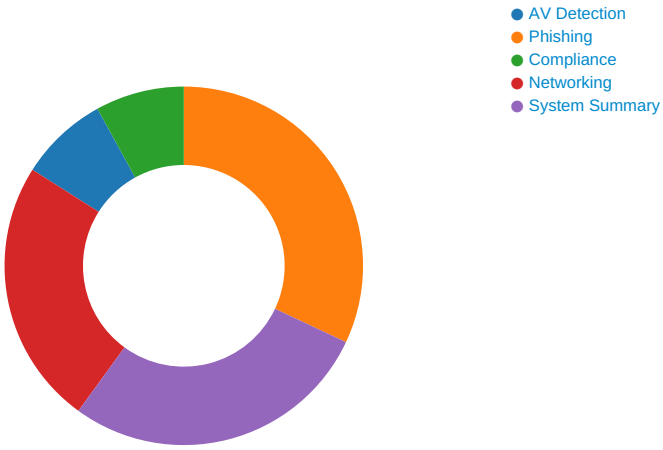
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\main[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

Antivirus detection for URL or domain

Phishing:

Phishing site detected (based on shot template match)

Yara detected HtmlPhish10

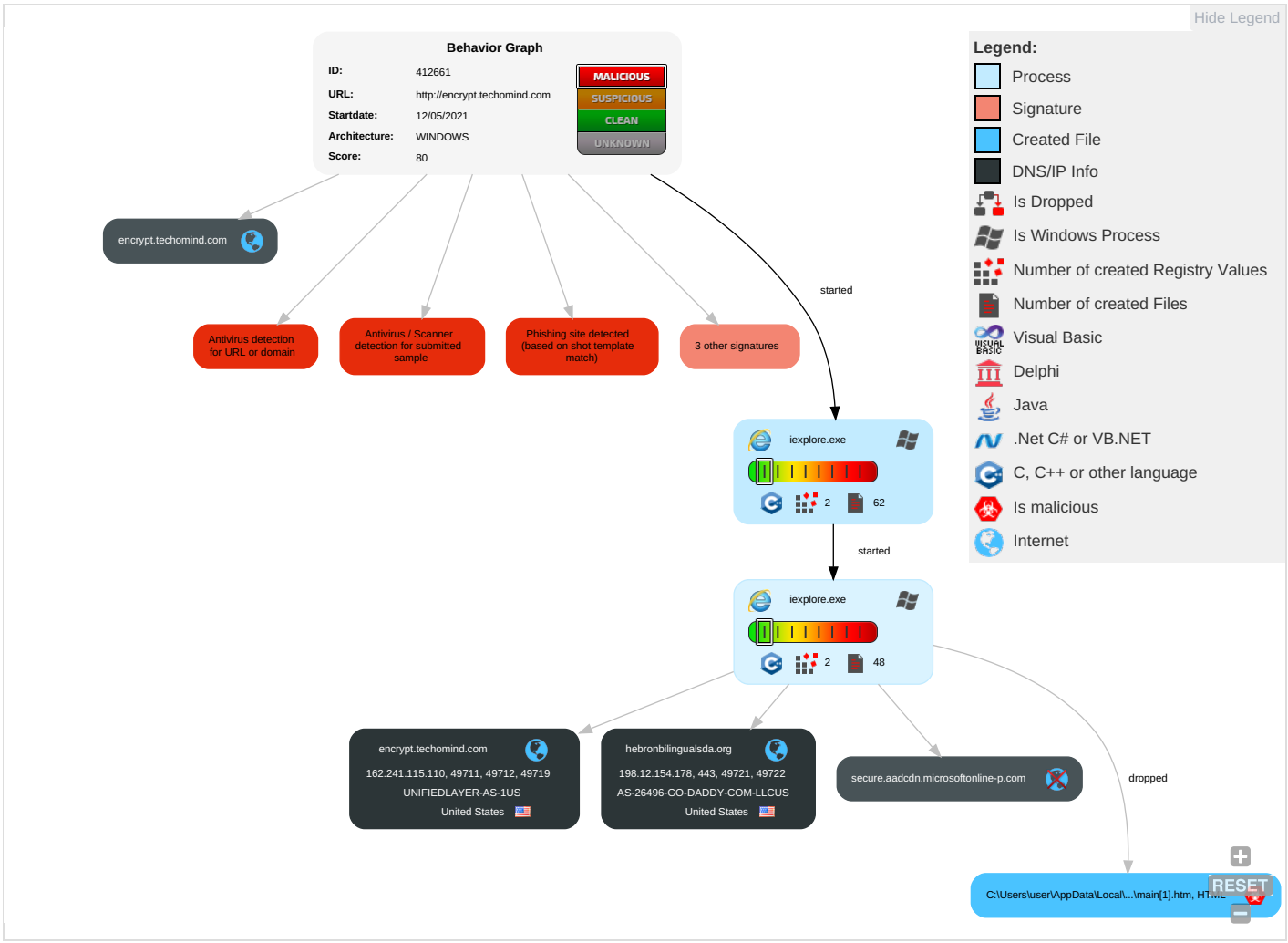
Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

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	Impa
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 Partit
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 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 4	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 3	SIM Card Swap		Carri Billin Fraud

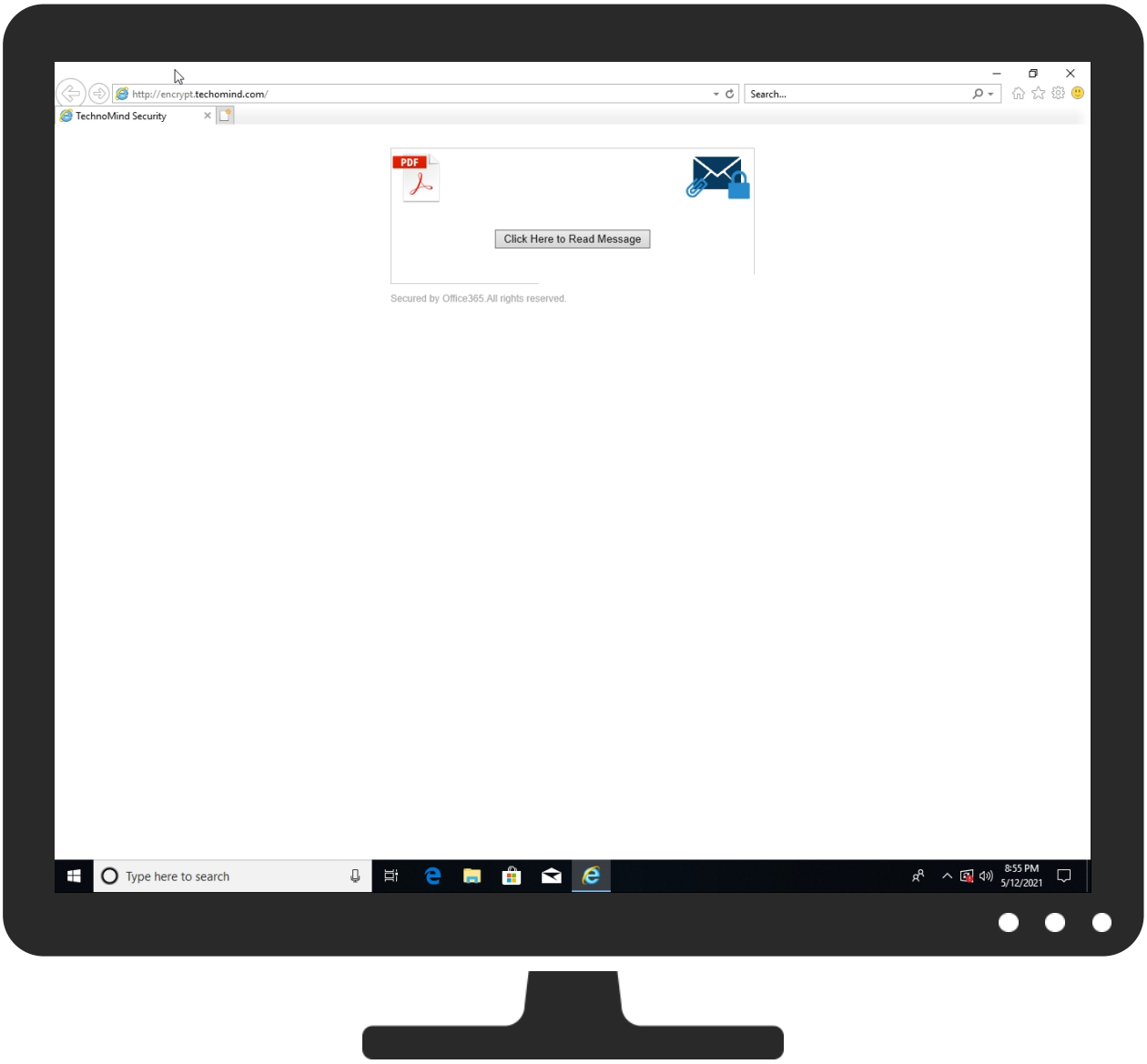
Behavior Graph



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://encrypt.techomind.com	0%	Avira URL Cloud	safe	
http://encrypt.techomind.com	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://encrypt.techomind.com/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://encrypt.techomind.com/wild.png	0%	Avira URL Cloud	safe	
http://https://hebronbilingualsda.org/content/main.html?accessToFile=validating&fileAccess=56662&encryptedC	0%	Avira URL Cloud	safe	
http://encrypt.techomind.com/Root	0%	Avira URL Cloud	safe	
http://https://hebronbilingualsda.org/content/cut.ico~	0%	Avira URL Cloud	safe	
http://encrypt.techomind.com/favicon.ico	0%	Avira URL Cloud	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.7135.7/content/images/picker_account_aad.svg?x=	0%	Avira URL Cloud	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.7135.7/content/images/ellipsis_grey.png?x=5bc25	0%	Avira URL Cloud	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.7135.7/content/images/ellipsis_white.png?x=0ad4	0%	Avira URL Cloud	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.7135.7/content/images/ellipsis_grey.svg?x=2b5d3	0%	Avira URL Cloud	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.7135.7/content/images/microsoft_logo.svg?x=ee5c	0%	Avira URL Cloud	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.7135.7/content/images/ellipsis_white.svg?x=5ac5	0%	Avira URL Cloud	safe	
http://encrypt.techomind.com/way.png	0%	Avira URL Cloud	safe	
http://encrypt.techomind.com/&TechnoMind	0%	Avira URL Cloud	safe	
http://https://hebronbilinguand.com/lsda.org/content/main.html?accessToFile=validating&fileAccess=56662&enc	0%	Avira URL Cloud	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.7135.7/content/images/microsoft_logo.png?x=ed9c	0%	Avira URL Cloud	safe	
http://encrypt.techomi	0%	Avira URL Cloud	safe	
http://https://hebronbilingualsda.org/content/cut.ico	0%	Avira URL Cloud	safe	
http://https://hebronbilingualsda.org/content/	0%	Avira URL Cloud	safe	
http://encrypt.techomind.com//content/main.html?accessToFile=validating&fileAccess=56662&encryptedCo	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
encrypt.techomind.com	162.241.115.110	true	false		unknown
hebronbilingualsda.org	198.12.154.178	true	false		unknown
secure.aadcdn.microsoftonline-p.com	unknown	unknown	false		unknown

Contacted URLs

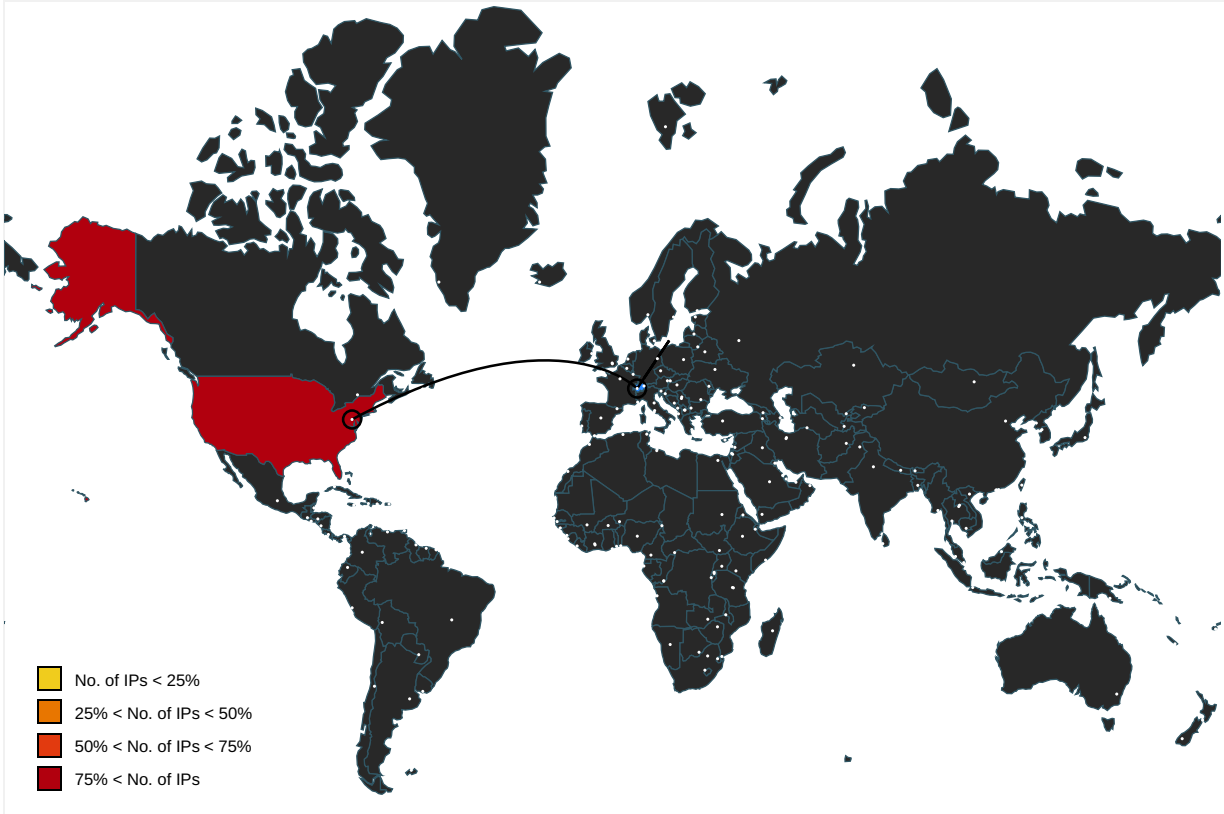
Name	Malicious	Antivirus Detection	Reputation
http://encrypt.techomind.com/wild.png	true	• Avira URL Cloud: safe	unknown
http://encrypt.techomind.com/favicon.ico	true	• Avira URL Cloud: safe	unknown
http://encrypt.techomind.com/	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://encrypt.techomind.com/way.png	true	• Avira URL Cloud: safe	unknown
http://https://hebronbilingualsda.org/content/main.html?accessToFile=validating&fileAccess=56662&encryptedCookie=5080b7079e42e7f7f42339337d7fbaa9&u=000142e8f0f0d64fe362ba89009a9da7&connecting=8ea008c13c68eba7937193ba001c13b4&phaseAccess=0eb7b8b7921971db486379d636704280&p=fb527d3e6d419408d9d7f0fb6644eb37	true		unknown
http://encrypt.techomind.com/	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://hebronbilingualsda.org/content/main.html?accessToFile=validating&fileAccess=56662&encryptedC	~DFCDF5FB740613BB71.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http://encrypt.techomind.com/Root	{06CF1659-B39F-11EB-90E4-ECF4BB862DED}.dat.2.dr	true	• Avira URL Cloud: safe	unknown
http://https://hebronbilingualsda.org/content/cut.ico~	imagestore.dat.3.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.7135.7/content/images/picker_account_aad.svg?x=	main[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.7135.7/content/images/ellipsis_grey.png?x=5bc25	main[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.7135.7/content/images/ellipsis_white.png?x=0ad4	main[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.7135.7/content/images/ellipsis_grey.svg?x=2b5d3	main[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.7135.7/content/images/microsoft_logo.svg?x=ee5c	main[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.7135.7/content/images/ellipsis_white.svg?x=5ac5	main[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://encrypt.techomind.com/&TechnoMind	~DFCDF5FB740613BB71.TMP.2.dr, {06CF1659-B39F-11EB-90E4-ECF4BB862DED}.dat.2.dr	true	• Avira URL Cloud: safe	unknown
http://https://hebronbilinguand.com/lsda.org/content/main.html?accessToFile=validating&fileAccess=56662&enc	{06CF1659-B39F-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.7135.7/content/images/microsoft_logo.png?x=ed9c	main[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://encrypt.techomi	{06CF1659-B39F-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://hebronbilingualsda.org/content/cut.ico	imagestore.dat.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://hebronbilingualsda.org/content/	3MODYROK.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://encrypt.techomind.com//content/main.html?accessToFile=validating&fileAccess=56662&encryptedCo	~DFCDF5FB740613BB71.TMP.2.dr	true	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.115.110	encrypt.techomind.com	United States		46606	UNIFIEDLAYER-AS-1US	false
198.12.154.178	hebronbilingualsda.org	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412661
Start date:	12.05.2021
Start time:	20:54:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://encrypt.techomind.com
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:	9
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:	mal80.phis.win@3/19@4/2
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://hebronbilingualsda.org/content/ • Browsing link: http://encrypt.techomind.com/
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 92.122.145.220, 52.255.188.83, 104.42.151.234, 88.221.62.148, 52.147.198.201, 172.217.23.106, 92.123.151.195, 23.57.80.111, 152.199.19.161, 20.82.210.154 • Excluded domains from analysis (whitelisted): store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, go.microsoft.com, e13761.dscg.akamaiedge.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, fs.microsoft.com, ajax.googleapis.com, ie9comview.vo.msecnd.net, secure.aadcdn.microsoftonline-p.com.edgekey.net, e1723.g.akamaiedge.net, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found. • VT rate limit hit for: http://encrypt.techomind.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.{06CF1657-B39F-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8531325930054259
Encrypted:	false
SSDEEP:	96:rLZ0ZG29WjIrtjIafjIDxMjvzojKjqfjRsX:rLZ0ZG29Wmtrf8xM4+GflsX
MD5:	AA4923F8AD51B4C877DD83098AD3502E
SHA1:	F2C96167CC87EAF3D59A429A8C144A118628B34A
SHA-256:	95BA0215ED1DF1A38E7EB36D7159AA6AC3AEBC21EC744D4658E22E6350318728
SHA-512:	ECA8F40D65536302D7ACEDA4481109997674603A2288B35CD32F6CBFA5DADA564DABBB98B0C7827EAF4EB8B395C2C6FBFCD65D8732A20D36A607597D9B6004FE
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\{06CF1659-B39F-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	54248
Entropy (8bit):	2.3869550237863826
Encrypted:	false
SSDEEP:	384:rcM2+tgQSLZbT25tODt690TDd3TtTjT+ToVi4+9MTqosf+9bpTs0:U2dyZpnqoQsTL

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{06CF1659-B39F-11EB-90E4-ECF4BB862DED}.dat	
MD5:	0FA80CF8279F9BDA3FA153A2D737D7DD
SHA1:	892C2BFDCCB21ABA964F595A48117188CF754358
SHA-256:	04FB442754B832AA31EE31C9368D95CFF6A406961C4D107EC7C6FA6BBB1681CE
SHA-512:	CC7C8A5162398339D7F8920BFCE4C5197FC91971926728BE1CDD0549446D774B3B6997DE7F849043BA034DE20062D52C9DF7FAC34C35B041DE8082010D5834B
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\{06CF165A-B39F-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5657852880496765
Encrypted:	false
SSDEEP:	48:IwpGcprYGwpahG4pQFGrapbSgHGQpK+PG7HpRiTGIpG:rvZAQz61BSIANT2A
MD5:	8756ACDE44534C698B73893813E894B9
SHA1:	978F83017F7AF73E2B27EFF9D82F76336BB19311
SHA-256:	CBF69A6F57DB5BD56D7872072C126CCA0DDDF61BB1DB0494F761149DF3CB70A2
SHA-512:	5DD52F895023C8E695EB47CE47117C56F0F27D864E6617D91CA344E3AD875C27DB73E68BA013103742111CB7AD97F5CE61ECF2576A8E5C76390D172395C39C1
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	8288
Entropy (8bit):	3.235816854929296
Encrypted:	false
SSDEEP:	48:Nj7w/6sOwH7nVj7wz/lO9dL/FknVj7wttRBwwkKK1mn/:1w/6s/wz/lC9SwTRyKK1C
MD5:	9877F0518F04C438910174E5117E097B
SHA1:	5BF923249DDACCD8703F36101CA9C3463D4027C0
SHA-256:	DBDD816B810E992A271048B980DB05425F5E7F34107CF77E32BD4BA5735BBC73
SHA-512:	A26794B7CF6A42E7A2FAAA9512330783656A228075730D4C1990BA33624B8C90D864E11DA79C6C21BB0528F27FB49376B688D68D4F46CD2CF7A321F6979787D8
Malicious:	false
Reputation:	low
Preview:	..h.t.t.p.s.:.//.h.e.b.r.o.n.b.i.l.i.n.g.u.a.l.s.d.a...o.r.g./.c.o.n.t.e.n.t./.c.u.t...i.c.o..... ....(... ...@..... .....(`.(..(..(..(..(..(..(..(..(..(..(..(..(..(..(..(..(..(.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ellipsis_grey[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):	3.8525277758130154
Encrypted:	false
SSDEEP:	24:t4CvnAVRfFArf1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUV0Uv6f1QqCWbVHTVeUVx:fn1r1QqC4GuiHFXS1QqCWRHQ3V1QqCWz
MD5:	2B5D393DB04A5E6E1F739CB266E65B4C
SHA1:	6A435DF5CAC3D58CCAD655FE022CCF3DD4B9B721
SHA-256:	16C3F6531D0FA5B4D16E82ABF066233B2A9F284C068C663699313C09F5E8D6E6
SHA-512:	3A692635EE8EBD7B15930E78D9E7E808E48C7ED3ED79003B8CA6F9290FA0E2B0FA3573409001489C00FB41D5710E75D17C3C4D65D26F9665849FB7406562A406
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://hebronbilingualsda.org/content/main_files/ellipsis_grey.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ellipsis_grey[1].svg	
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path fill="#777777" 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-.446.089,1.107,1.107,0,0,1,.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-.607A1.107,1.107,0,0,1,8,1.143,1.107,1.107,0,0,1,8.446,1.232,1.164,1.164,0,0,1,9.054,1.839,1.161,1.161,0,0,1,9.143,2.286,1.107,1.107,0,0,1,9.054,2.732,1.164,1.164,0,0,1,8.446,3.339,1.161,1.161,0,0,1,8,3.429,1.107,1.107,0,0,1,7.554,3.339,1.164,1.164,0,0,1,6.946,2.732,1.161,1.161,0,0,1,6.857,2.286,1.107,1.107,0,0,1,6.946,1.839,1.164,1.164,0,0,1,7.554,1.232,1.107,1.107,0,0,1,8,1.143M8,0a8,8,0,1,0,8,8A8,8,0,0,0,8,0Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	86659
Entropy (8bit):	5.36781915816204
Encrypted:	false
SSDEEP:	1536:YNhEyjjTikEJO4edXXe9J578go6MWX2xkj8e4c4j2ll2AckaXEP6n15HZ+FhFcQ7:uxc2yjx4j2uX/kcQDU8Cu9
MD5:	C9F5AEECA3AD37BF2AA006139B935F0A
SHA1:	1055018C28AB41087EF9CCEFE411606893DABEA2
SHA-256:	87083882CC6015984EB0411A99D3981817F5DC5C90BA24F0940420C5548D82DE
SHA-512:	DCFF2B5C2B8625D3593A7531FF4DDCD633939CC9F7ACFEB79C18A9E6038FDAA99487960075502F159D44F902D965B0B5AED32B41BFA66A1DC07D85B5D5152B8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/3.2.1/jquery.min.js
Preview:	/*! jQuery v3.2.1 | (c) JS Foundation and other contributors | jquery.org/license */!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.2.1",r=function(a,b){return new r.fn.init(a,b)},s=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,t=/^-ms-/,u=/-([a-z])/g,v=function(a,b){return b.toUpperCase()};r.fn=r.prototype={jquery:q,constructor:r,length:0,toArray:function(){return f.call(this)},get:function(a){return null==a?f.call(this):a<0?this[a+this.length]:this[a]},pushStack:function(a){var

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\main[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	12673
Entropy (8bit):	5.286805301183663
Encrypted:	false
SSDEEP:	384:MMy10FdZKsmlKvtyDJy9/QKcWHMxKp4xKrLtOOYwgfVEjgxMw4M:9ey0ywTL
MD5:	4E854F15167062E24CEC09BA4AB67830
SHA1:	3773C2228152E539BB0F4FE9DAEB5D4895CC244B
SHA-256:	D659FD9ACC9C14613363F06433707EAAD9BBD6276D29CB342C788C62BEA40D3C
SHA-512:	9D2EDDCADB706D7B3652C924AB2AA12972F43321FD3F4ACFEAFE8E706E12F45CE74CB4EAADBDCF3B1EFEBFBF18600C62BFF300D5F72685CAD7729047BA5CE9CA
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\main[1].htm, Author: Joe Security
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Frameset//EN" "http://www.w3.org/TR/html4/frameset.dtd">.<HTML>.<head>.<TITLE>Office 365 for Business</TITLE>.<META HTTP-EQUIV="content-type" content="text/html; charset=UTF-8">.</head>....<meta http-equiv="X-UA-Compatible" content="IE=edge">.....<meta http-equiv="Pragma" content="no-cache">...<meta http-equiv="Expires" content="-1">...<meta name="PageID" content="documentId">...<meta name="SiteID" content="./,inv,.luesaghunbmjgfjk">...<meta name="ReqLC" content="1033">...<meta name="LocLC" content="en-US">...<link rel="shortcut icon" href='cut.ico'>...<link href="./main_files/converged.login.min.css" rel="stylesheet">...<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.2.1/jquery.min.js"></script>..</head>...<body data-bind="defineGlobals: ServerData, bodyCssClass" class="cb" style="display: block;">... ....</head><body style="visibility: visible;" onload="unhideBody()" bgproperties="fixed" background="Sign in_files/oval.png"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\way[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 90 x 68, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	3775
Entropy (8bit):	7.882480508533676
Encrypted:	false
SSDEEP:	96:Gfb888888Saq9YGlXFr4Eg44lFr3+yIvSdo3E3EbI:GD888888SLGGltg44/+yqE0M
MD5:	CCC837EE4BE44D6FC11F13282710CE27
SHA1:	AED8345218C15FDA81959CCF00E8A004A0C6CAB1
SHA-256:	DC085EA274CCEA414B19BA730080659BACA694F0982F69FEB85BF55AA87E3129
SHA-512:	EA48CC84F3A5FCEA83652222BA8853B53818E9141A90D1EA0029785E11F38737B383FF1733669E86B3CAE88D4ACA3EC40B22AAE63F2F3D6D2E8D0E1B20EEE9EB

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\way[1].png	
Malicious:	false
Reputation:	low
IE Cache URL:	http://encrypt.techomind.com/way.png
Preview:	.PNG.....IHDR...Z...D.....t".....sRGB.....YiTXtXML:com.adobe.xmp.....<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="XMP Core 5.4.0">. <rdf:RDF xmlns:rdf= "http://www.w3.org/1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about="". xmlns:tiff="http://ns.adobe.com/tiff/1.0/">. <tiff:Orientation>1</tiff:Orient ation>. </rdf:Description>. </rdf:RDF>.</x:xmpmeta>.L.'Y....IDATx...xS....m.&..PZ...."`.....&Z.W."."....d.....=@...@....OEY....b.R.R@hYl..M.ys.vno.6)M...|..sg.g.{.3g..;..... .....P....z...._..V...B.a]6. .(.....Uvs.{.9.Y.7.-;....o....#..e.a.A,IF.y....[..R..&.._..0>.....O.j..w..b;E.;.K.{z*a..:....L1....g7h.Z..fdA.s..I..ua.....6.K../i..K.%....^sh7hN.BN..'>e. {.g.._..^ZO..^....g.\).FA.%/!.....))..|....5....Q...t..... ...E.e^r.....K.-%..'/6....-aH.n.I....i.....L. ...#f*.K.*.S@..G3/...riw.](..... .K^.yt.~..L.1..A..m.S.p.h..j....<...../N...~_...:e B....iK..../.}..hL.&.q*h...h.u.R..E..+\@t.^

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\wild[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 61 x 63, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	3808
Entropy (8bit):	7.865556791496107
Encrypted:	false
SSDEEP:	96:1eq29skAdr/SViDXEKYI39zc/AE5N2J3+:WoucDXlXzcp5Ny3+
MD5:	CFE8396A4F2E8D1202F317E4FE76CAC3
SHA1:	9C55C8EB46D68C37FF216B9F53F9A5F3A257FF3F
SHA-256:	5E2EA92B0B528068DA05C981358318141B5F4CF8AF66F0E63EB0AB59E8F1C6F7
SHA-512:	1640B3B38961A3F75232C9674B8ADCF179C69D50EBD14F47774EE216D7F45ADCD109488483EC66A1B8C8504730378E10D71A5086FD74D33AA99AF93E3CBDCDF
Malicious:	false
Reputation:	low
IE Cache URL:	http://encrypt.techomind.com/wild.png
Preview:	.PNG.....IHDR...=...?.....W.....sRGB.....iTXtXML:com.adobe.xmp.....<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="XMP Core 5.4.0">. <rdf:RDF xmlns:rdf= "http://www.w3.org/1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about="". xmlns:tiff="http://ns.adobe.com/tiff/1.0/">. <tiff:Compression>5</tiff:Compre ssion>. <tiff:PhotometricInterpretation>2</tiff:PhotometricInterpretation>. <tiff:Orientation>1</tiff:Orientation>. </rdf:Description>. </rdf:RDF>.</x:xmpmet a>...2.....IDATh..Z{l....}..w.._u..;.....4P ...H.....G....?Ji*UmA}..J@.....DK.....R.@.$!..I .... ..yw.....x...-..#{..o..o..fvv.$....._@...:K.e..il....".4...(_..f.....P($..g.;.D"a.&.....El2....7 .).u,....'kjj".H9.....u.r GG....3.|^.h!lb8q.9.@T...2..VUbY.=11.#....J.j..N.].?x_..=.=g...@3....,...QV5>t....Tb....;...in.,....:.....64.....V...FOU..O.&...`.j...A ()M.l.D..4.$.....CCsjjb.X9..- ...d+ ..qR.....!...1>e"...u.8.R..0....m.....t.&6...I....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\converged.login.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	87707
Entropy (8bit):	5.312405825151679
Encrypted:	false
SSDEEP:	1536:QpHDglHuhw+E3vUB+2PWrA2XU6BMxoAFi262:lB6
MD5:	CADB60F6A832628A4048ED795CE60E42
SHA1:	0BBE73405D5CA9608788BF4A7C03BE7B4932FE68
SHA-256:	A8E954FC9668172A94B5E7D74EFCA982D6ABD6891D0457E3D859C99018087FFF
SHA-512:	729F068E4C9D146A957F6129FC4C407BF887C07C1D76EE4441EC0DA749B794B1D3CCA82766E4B7E4634DA937DCB071F43427616A3D953A39B6131166E9422226
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://hebronbilingualsda.org/content/main_files/converged.login.min.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 Tw Inc..Permission is hereby granted, free of charge, to any person

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\ellipsis_white[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:	B9135D934B9EA50B51BB0316E383B114C8F24DFE75FEF11DCBD1C96170EA59202F6BAFE11AAF534CC2F4ED334A8EA4DBE96AF2504130896D6203BFD2DA6913 F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\ellipsis_white[1].svg	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://hebronbilingualsda.org/content/main_files/ellipsis_white.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-.089A1.107,1.107,0,0,1,9.054,8,1.107,1.107,0,0,1,8,6.857m6.857,0a1.107,1.107,0,0,1,.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-.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607A1.107,1.107,0,0,1,14.857,8,1.107,1.107,0,0,1,14.857,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\oval[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1582 x 1055, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	271219
Entropy (8bit):	7.91482289641543
Encrypted:	false
SSDEEP:	6144:ZM17xgwBmZA+5QgRULy4jmsC/RnLrCVSvMhfFAsLz/o:Zm7xgimZp1RV9xeVcefFlnA
MD5:	FD7EE42C722A392D8149A11BAF66495C
SHA1:	3482B8B987851BD70761A3AE51FC1FDB4009FA36
SHA-256:	DDB6B5706F83F5A11D4DE018B5B1D40164EE2703F95E4ED6BA93A656F6B17EDD
SHA-512:	82508D2C0FCF0BBB52CBB0053C59926ABACF78ACD0361C45C3C88219A7C5B6F1760016B55B582DC5A9BAC65002D060FCBD4C560DB914EAB9FC0B04840E4E5D3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://hebronbilingualsda.org/content/Sign%20in_files/oval.png
Preview:	.PNG........IHDR.....e.o....iCCPICC Profile..8..U]h.U.>.sg#$.Sl4.t.?.%..V4.....6n.I6.".d.....83...OEP\|1..... (...>./..%.. (>...P..;3.i...e.\|..{.g...X.....-.2.s...=+.....WQ.+].L.6O.w.[.C.{_.....F.. q.b.....U.v.z...?.Z..b.1@./z..c..s>~.if.,...USj.....F..1.._.Mj...b.u..p.a..m.h..m...>..a\.+5%..Q.K...F...km}.....?.....D\.....!~.6.,.-..7..S.....v.5Z..;....[...r.mS.....5..{yD...yH.}r.9..\|..-.....FA.....J...j..I.....[/.]m...K..7..K....R..D..r..Y..Q..O.-....Q...\|.\|.6.....(.0...MX..d(@....h....2....._.f....<.:....._....*d.>.....e.\c.?~,7.?&. ...^2I..q2."y.<M.....d...JlE^<7....3R..E.9...`.3*L\S.,...#.)..]...._.\.,7Q.....W.._...2.+.j....W.r.Z..L..lXswU.m.....q..W.F~....]<Yo..F....j.V.N.D...,.'}(...}.}.}.}.]..;....p.s_..j..Z.{.y..g.k.J!#l...r.6.Qa2.'..cBQ...../.=..c...\..V.....M.UUT.p.).VoM8.A..$Cd..6T..W.".O.Ri.S;S....A....v.m.....n.R..c.}.Y.:n....wK.b..6*.....L.hS..mZ.....2...[.G...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\picker_account_aad[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	756
Entropy (8bit):	4.879179443781471
Encrypted:	false
SSDEEP:	12:t4pb8WsQKvkBWSfYcW3ffBfYfomQO1a7aajR2F1hgWSnuCNSganii7v/NPujARqj:t4pb8WvKMTfY3ffBfYfomQO1eXjR2oug
MD5:	9DE70D1C5191D1852A0D5AAC28B44A6C
SHA1:	F4F64F5CBDBE6D1115C10A7F9CCB8828E6B67CAE
SHA-256:	5D3357BD875B7335ACE42E8EE3A64578E4253BED1A4E279109DE403EEDAE3A69
SHA-512:	CAC13FC2FE30E10772008F2AFF70FCA031EA9918E1F8C5C8B91CB9E79463383183406EFAADF89360DE3A08573FCDF2716C14DA6411E24B7E260B96AF84F0076
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.7135.7/content/images/picker_account_aad.svg?x=9de70d1c5191d1852a0d5aac28b44a6c
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="48" height="48" viewBox="0 0 48 48"><title>assets</title><circle cx="24" cy="24" r="24" fill="#e6e6e6"/><path d="M34,35V14a2.938,2.938,0,0,0-3-3H27V8l2-1L27.948,5.638,24,8,20.07,5.648,19,7l2,1v3H17a2.938,2.938,0,0,0-3,3V35a2.938,2.938,0,0,0,3,3H31A2.938,2.938,0,0,0,34,35Zm-3,1H17a.979.979,0,0,0,1-1-1V14a.979.979,0,0,0,1,1-1h6V10h2v3h6a.979.979,0,0,1,1,1V35A.979.979,0,0,1,31,36Z" fill="#404040"/><path d="M26.766,25.42a4.432,4.432,0,1,0-5.533,0A6.237,6.237,0,0,0,0,17.765,31h1.653a4.582,4.582,0,1,1,9.165,0h1.653A6.237,6.237,0,0,0,26.766,25.42Zm-5.546-3.435A2.779,2.779,0,1,1,24,24.765,2.783,2.783,0,0,1,21.221,21.985Z" fill="#404040"/><rect x="21" y="14" width="6" height="2" rx="1" ry="1" fill="#404040"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\3MODYROK.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1547
Entropy (8bit):	5.0599895867122555
Encrypted:	false
SSDEEP:	48:0WWSoX8CMtatnHiBu5C62KLs5C2lfMsMG9M7:6SYMtatnCsrTW96bZ7
MD5:	C502CAB1FA3973A749F60608C2FC3605
SHA1:	B66C3960943C14C955A79683E148380632EE708A
SHA-256:	933A8AE0F27D4B101EB250D98DE39962CFE574DDDED155B47A0CE3F3B6586B22
SHA-512:	F53EC6E2D443504A8768787C65CB0251050DA2A057F9399E51DB77E0308D97B7352C5CC93417F859E1DBE01741A7BB9FEA7853FAB44825391E017D150590BDB5
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\3MODYROK.htm	
Reputation:	low
IE Cache URL:	http://encrypt.techomind.com/
Preview:	<!doctype public "-//wapforum//dtd wml 1.2//en">..<html>..<head>..<TITLE>TechnoMind Security</TITLE>..<META HTTP-EQUIV="content-type" content="text/html; charset=UTF-8">..</head>....<body style="font-size: 5px; font-family: arial; ">..<table style="width:50px; border-collapse: collapse; margin-left: auto; margin-right: auto;"> .. <tbody><tr><td style="padding-top: 20px;">.. <table style="padding-top: 10px; padding-left: 10px; padding-right: 10px; padding-bottom: 20px; background-color: #FFFFFF; border:1px solid #CCCCCC; color:#000000; width: 450px;">.. <tbody><tr><td><img src='wild.png' border="0"> </td>.. <td align="right"><img src='way.png'></td>.. </tr>.. <tr><td colspan="2" style="font-size: 12px; padding-top: 30px; text-align: center;"> <button>Click Here to Read Message</button>.. .. .. .. <tr><td colspan="2" styl

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cut[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 3 icons, 32x32, 32 bits/pixel, 24x24, 32 bits/pixel
Category:	downloaded
Size (bytes):	7886
Entropy (8bit):	3.1280056112498884
Encrypted:	false
SSDEEP:	24:i7xEfZFssEcdSsssss9udddSsssssss8VpddddSssssssssss4cddddddyssssF:gu6sOwH0/lO9dL/FLRBwwkKK1V
MD5:	604ADFB53677B5CA4F910FFB131B3E7C
SHA1:	5F1A0FB4E4AD3707E591CE16352158263488ED70
SHA-256:	24638331466A52BB66F912090E7A9CC9E3DF2236E39C187C9409104526B472B0
SHA-512:	35F618F42ADFEE6D1335C67F729C298789419FE2930371A91683F60481794488DFAF15B572E6FC1BE70833EF12DFE57432725F6336B6B73DCFB52596F57F30A5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://hebronbilingualsda.org/content/cut.ico
Preview:	....6......... .... .h...f...(... ...@..... ....(`.(..(p.....................

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\microsoft_logo[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://hebronbilingualsda.org/content/main_files/microsoft_logo.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392,1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47.081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0,0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.611,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.952,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

C:\Users\user\AppData\Local\Temp\~DF08B42D9D3081252A.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4795904381147373
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loGF9loq9lWDGjaB7jqEN:kBqoIlTDIyvqK
MD5:	EC3578716C165A1C494325D9F411F0DF
SHA1:	B4F8E0D5E567F9F07FE7834A4380321959B7B092
SHA-256:	A1CF640CDF26B2BDD3BC73877B8ED4B979B0756F2F948EEC62AF25E24740BFD6
SHA-512:	33C2A8FCD9F6671B91EF303796AE9B27FDF51AE39D42BC820A8EEB95D7BA500C90947CD763CB5AFC402DBF492DE5527945B532A29EC35FD02C2E74AAED88E 85
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DF08B42D9D3081252A.TMP	
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFCDF5FB740613BB71.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	57037
Entropy (8bit):	1.3249041476253953
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+mg6TgYj55ThpiTxTDd3TtTjT+TvfTKhZaT+TqqTjpT:SKFZpnqTQUqdZ
MD5:	D62216803A165165F63E14C26D9B1CB8
SHA1:	8072822CD03CAC75F12D93B3AA4179100CDAB212
SHA-256:	8049CE31801D93574B639C3382DA3B20E6FCD6C1FDA752A1FA0694728BD2287F
SHA-512:	87B19AA0AB8CF68B65B025696DD07B0EC8D6E27EB6112072E8629B1DEEBFC35A2940229CBD29E6FBBC60A0D886863AAE93108F640ED6C0C8CBF4D204353433 A9
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

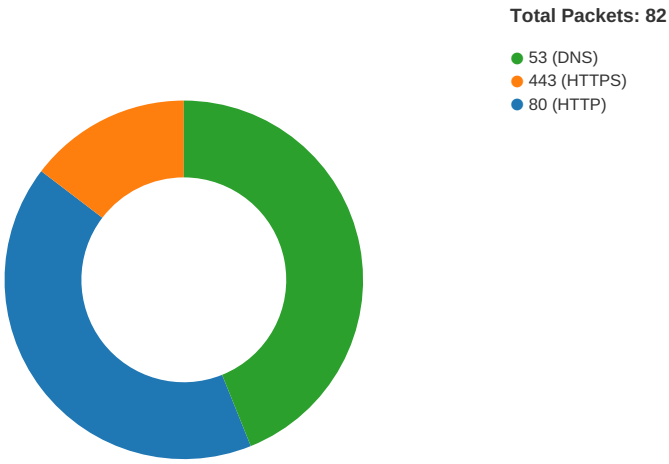
C:\Users\user\AppData\Local\Temp\~DFF7CEDCC2DA9C786D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.30164564897849105
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAR:kBqoxxJhHWSVSEab
MD5:	23BF0C805BF41A7E5906C218903EFE84
SHA1:	AAC4FD7376E82BC093119C349680332E8F578C47
SHA-256:	8D25516FEAC0F5D5BC965D588E963DF252A79E88659F755373E56C528568EA30
SHA-512:	56BCE027F9AD53D7D7F69C3C965CE2F39422C9F4FF31E9652DA95277DDB28EEF018E81C69E8319A06E5EF41B33F7A4049C152940B1A8E1BA7E5980FBF3BED71 D
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:55:19.169681072 CEST	49712	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:19.169711113 CEST	49711	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:19.332251072 CEST	80	49712	162.241.115.110	192.168.2.3
May 12, 2021 20:55:19.332993984 CEST	49712	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:19.333013058 CEST	49712	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:19.333017111 CEST	80	49711	162.241.115.110	192.168.2.3
May 12, 2021 20:55:19.333105087 CEST	49711	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:19.496316910 CEST	80	49712	162.241.115.110	192.168.2.3
May 12, 2021 20:55:19.497272968 CEST	80	49712	162.241.115.110	192.168.2.3
May 12, 2021 20:55:19.497304916 CEST	80	49712	162.241.115.110	192.168.2.3
May 12, 2021 20:55:19.497373104 CEST	49712	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:19.497406006 CEST	49712	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:19.583978891 CEST	49712	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:19.585012913 CEST	49711	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:19.748285055 CEST	80	49712	162.241.115.110	192.168.2.3
May 12, 2021 20:55:19.748313904 CEST	80	49712	162.241.115.110	192.168.2.3
May 12, 2021 20:55:19.748326063 CEST	80	49712	162.241.115.110	192.168.2.3
May 12, 2021 20:55:19.748334885 CEST	80	49712	162.241.115.110	192.168.2.3
May 12, 2021 20:55:19.748413086 CEST	49712	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:19.748446941 CEST	49712	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:19.749356031 CEST	80	49711	162.241.115.110	192.168.2.3
May 12, 2021 20:55:19.749896049 CEST	80	49711	162.241.115.110	192.168.2.3
May 12, 2021 20:55:19.749918938 CEST	80	49711	162.241.115.110	192.168.2.3
May 12, 2021 20:55:19.749931097 CEST	80	49711	162.241.115.110	192.168.2.3
May 12, 2021 20:55:19.749946117 CEST	80	49711	162.241.115.110	192.168.2.3
May 12, 2021 20:55:19.749991894 CEST	49711	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:19.752753973 CEST	49711	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:19.938215017 CEST	49712	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:20.101005077 CEST	80	49712	162.241.115.110	192.168.2.3
May 12, 2021 20:55:20.101037025 CEST	80	49712	162.241.115.110	192.168.2.3
May 12, 2021 20:55:20.101049900 CEST	80	49712	162.241.115.110	192.168.2.3
May 12, 2021 20:55:20.101062059 CEST	80	49712	162.241.115.110	192.168.2.3
May 12, 2021 20:55:20.101078033 CEST	80	49712	162.241.115.110	192.168.2.3
May 12, 2021 20:55:20.101094007 CEST	80	49712	162.241.115.110	192.168.2.3
May 12, 2021 20:55:20.101109028 CEST	80	49712	162.241.115.110	192.168.2.3
May 12, 2021 20:55:20.101120949 CEST	80	49712	162.241.115.110	192.168.2.3
May 12, 2021 20:55:20.101133108 CEST	80	49712	162.241.115.110	192.168.2.3
May 12, 2021 20:55:20.101147890 CEST	80	49712	162.241.115.110	192.168.2.3
May 12, 2021 20:55:20.101185083 CEST	49712	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:20.101253033 CEST	49712	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:20.121684074 CEST	49712	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:20.121753931 CEST	49712	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:20.263264894 CEST	80	49712	162.241.115.110	192.168.2.3
May 12, 2021 20:55:20.263287067 CEST	80	49712	162.241.115.110	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:55:20.263377905 CEST	49712	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:20.264995098 CEST	49712	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:24.755240917 CEST	80	49711	162.241.115.110	192.168.2.3
May 12, 2021 20:55:24.755393028 CEST	49711	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:36.895139933 CEST	49719	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:37.053952932 CEST	80	49719	162.241.115.110	192.168.2.3
May 12, 2021 20:55:37.054163933 CEST	49719	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:37.073615074 CEST	49719	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:37.232345104 CEST	80	49719	162.241.115.110	192.168.2.3
May 12, 2021 20:55:37.233072042 CEST	80	49719	162.241.115.110	192.168.2.3
May 12, 2021 20:55:37.233189106 CEST	80	49719	162.241.115.110	192.168.2.3
May 12, 2021 20:55:37.233205080 CEST	49719	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:37.233212948 CEST	80	49719	162.241.115.110	192.168.2.3
May 12, 2021 20:55:37.233244896 CEST	80	49719	162.241.115.110	192.168.2.3
May 12, 2021 20:55:37.233273983 CEST	49719	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:37.233290911 CEST	80	49719	162.241.115.110	192.168.2.3
May 12, 2021 20:55:37.233309031 CEST	80	49719	162.241.115.110	192.168.2.3
May 12, 2021 20:55:37.233314991 CEST	49719	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:37.233326912 CEST	80	49719	162.241.115.110	192.168.2.3
May 12, 2021 20:55:37.233339071 CEST	80	49719	162.241.115.110	192.168.2.3
May 12, 2021 20:55:37.233346939 CEST	80	49719	162.241.115.110	192.168.2.3
May 12, 2021 20:55:37.233351946 CEST	49719	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:37.233360052 CEST	80	49719	162.241.115.110	192.168.2.3
May 12, 2021 20:55:37.233417034 CEST	49719	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:37.233426094 CEST	49719	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:37.233762980 CEST	49719	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:37.233794928 CEST	49719	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:37.392118931 CEST	80	49719	162.241.115.110	192.168.2.3
May 12, 2021 20:55:37.392146111 CEST	80	49719	162.241.115.110	192.168.2.3
May 12, 2021 20:55:37.392287970 CEST	49719	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:37.392332077 CEST	49719	80	192.168.2.3	162.241.115.110
May 12, 2021 20:55:38.670916080 CEST	49721	443	192.168.2.3	198.12.154.178
May 12, 2021 20:55:38.671294928 CEST	49722	443	192.168.2.3	198.12.154.178
May 12, 2021 20:55:38.855416059 CEST	443	49722	198.12.154.178	192.168.2.3
May 12, 2021 20:55:38.855504036 CEST	49722	443	192.168.2.3	198.12.154.178
May 12, 2021 20:55:38.859340906 CEST	443	49721	198.12.154.178	192.168.2.3
May 12, 2021 20:55:38.859483957 CEST	49721	443	192.168.2.3	198.12.154.178
May 12, 2021 20:55:38.859858036 CEST	49722	443	192.168.2.3	198.12.154.178
May 12, 2021 20:55:38.860090017 CEST	49721	443	192.168.2.3	198.12.154.178
May 12, 2021 20:55:39.043761969 CEST	443	49722	198.12.154.178	192.168.2.3
May 12, 2021 20:55:39.044406891 CEST	443	49722	198.12.154.178	192.168.2.3
May 12, 2021 20:55:39.044425964 CEST	443	49722	198.12.154.178	192.168.2.3
May 12, 2021 20:55:39.044455051 CEST	443	49722	198.12.154.178	192.168.2.3
May 12, 2021 20:55:39.044471025 CEST	443	49722	198.12.154.178	192.168.2.3
May 12, 2021 20:55:39.044487953 CEST	49722	443	192.168.2.3	198.12.154.178
May 12, 2021 20:55:39.044511080 CEST	49722	443	192.168.2.3	198.12.154.178
May 12, 2021 20:55:39.044552088 CEST	49722	443	192.168.2.3	198.12.154.178
May 12, 2021 20:55:39.046000004 CEST	443	49722	198.12.154.178	192.168.2.3
May 12, 2021 20:55:39.046076059 CEST	49722	443	192.168.2.3	198.12.154.178
May 12, 2021 20:55:39.048530102 CEST	443	49721	198.12.154.178	192.168.2.3
May 12, 2021 20:55:39.049149990 CEST	443	49721	198.12.154.178	192.168.2.3
May 12, 2021 20:55:39.049168110 CEST	443	49721	198.12.154.178	192.168.2.3
May 12, 2021 20:55:39.049201012 CEST	49721	443	192.168.2.3	198.12.154.178
May 12, 2021 20:55:39.049215078 CEST	443	49721	198.12.154.178	192.168.2.3
May 12, 2021 20:55:39.049225092 CEST	49721	443	192.168.2.3	198.12.154.178
May 12, 2021 20:55:39.049237013 CEST	443	49721	198.12.154.178	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:55:10.295912027 CEST	64938	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:10.354160070 CEST	53	64938	8.8.8.8	192.168.2.3
May 12, 2021 20:55:10.357953072 CEST	60152	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:10.408879995 CEST	53	60152	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:55:12.596694946 CEST	57544	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:12.648274899 CEST	53	57544	8.8.8.8	192.168.2.3
May 12, 2021 20:55:13.608371019 CEST	55984	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:13.663625956 CEST	53	55984	8.8.8.8	192.168.2.3
May 12, 2021 20:55:14.916565895 CEST	64185	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:14.965711117 CEST	53	64185	8.8.8.8	192.168.2.3
May 12, 2021 20:55:16.069217920 CEST	65110	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:16.118307114 CEST	53	65110	8.8.8.8	192.168.2.3
May 12, 2021 20:55:17.557293892 CEST	58361	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:17.622308969 CEST	53	58361	8.8.8.8	192.168.2.3
May 12, 2021 20:55:17.815946102 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:17.866380930 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 20:55:18.954871893 CEST	60831	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:18.970432997 CEST	60100	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:19.006604910 CEST	53	60831	8.8.8.8	192.168.2.3
May 12, 2021 20:55:19.157399893 CEST	53	60100	8.8.8.8	192.168.2.3
May 12, 2021 20:55:21.364834070 CEST	53195	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:21.416445971 CEST	53	53195	8.8.8.8	192.168.2.3
May 12, 2021 20:55:22.694133043 CEST	50141	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:22.744496107 CEST	53	50141	8.8.8.8	192.168.2.3
May 12, 2021 20:55:30.071532011 CEST	53023	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:30.120254993 CEST	53	53023	8.8.8.8	192.168.2.3
May 12, 2021 20:55:30.929574013 CEST	49563	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:30.979867935 CEST	53	49563	8.8.8.8	192.168.2.3
May 12, 2021 20:55:32.203494072 CEST	51352	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:32.252578974 CEST	53	51352	8.8.8.8	192.168.2.3
May 12, 2021 20:55:33.476962090 CEST	59349	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:33.527564049 CEST	53	59349	8.8.8.8	192.168.2.3
May 12, 2021 20:55:36.712088108 CEST	57084	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:36.891705036 CEST	53	57084	8.8.8.8	192.168.2.3
May 12, 2021 20:55:37.800879002 CEST	58823	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:37.852659941 CEST	53	58823	8.8.8.8	192.168.2.3
May 12, 2021 20:55:38.578542948 CEST	57568	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:38.668457031 CEST	53	57568	8.8.8.8	192.168.2.3
May 12, 2021 20:55:39.011651039 CEST	50540	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:39.060482025 CEST	53	50540	8.8.8.8	192.168.2.3
May 12, 2021 20:55:39.591609955 CEST	54366	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:39.601068020 CEST	53034	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:39.659210920 CEST	53	54366	8.8.8.8	192.168.2.3
May 12, 2021 20:55:39.659343958 CEST	53	53034	8.8.8.8	192.168.2.3
May 12, 2021 20:55:40.121537924 CEST	57762	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:40.171147108 CEST	53	57762	8.8.8.8	192.168.2.3
May 12, 2021 20:55:40.939543009 CEST	55435	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:40.988676071 CEST	53	55435	8.8.8.8	192.168.2.3
May 12, 2021 20:55:46.554241896 CEST	50713	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:46.613457918 CEST	53	50713	8.8.8.8	192.168.2.3
May 12, 2021 20:55:47.522217035 CEST	56132	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:47.572046995 CEST	53	56132	8.8.8.8	192.168.2.3
May 12, 2021 20:55:48.335844994 CEST	58987	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:48.393007994 CEST	53	58987	8.8.8.8	192.168.2.3
May 12, 2021 20:55:48.528588057 CEST	56132	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:48.577445984 CEST	53	56132	8.8.8.8	192.168.2.3
May 12, 2021 20:55:49.371742010 CEST	58987	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:49.436201096 CEST	53	58987	8.8.8.8	192.168.2.3
May 12, 2021 20:55:49.528723955 CEST	56132	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:49.577887058 CEST	53	56132	8.8.8.8	192.168.2.3
May 12, 2021 20:55:50.409593105 CEST	58987	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:50.471972942 CEST	53	58987	8.8.8.8	192.168.2.3
May 12, 2021 20:55:50.553781986 CEST	56579	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:50.619069099 CEST	53	56579	8.8.8.8	192.168.2.3
May 12, 2021 20:55:51.609132051 CEST	56132	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:51.658549070 CEST	53	56132	8.8.8.8	192.168.2.3
May 12, 2021 20:55:52.402791023 CEST	58987	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:52.460412025 CEST	53	58987	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:55:55.622617960 CEST	56132	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:55.671366930 CEST	53	56132	8.8.8.8	192.168.2.3
May 12, 2021 20:55:56.418653965 CEST	58987	53	192.168.2.3	8.8.8.8
May 12, 2021 20:55:56.476162910 CEST	53	58987	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 20:55:18.970432997 CEST	192.168.2.3	8.8.8.8	0xc334	Standard query (0)	encrypt.techomind.com	A (IP address)	IN (0x0001)
May 12, 2021 20:55:36.712088108 CEST	192.168.2.3	8.8.8.8	0x978e	Standard query (0)	encrypt.techomind.com	A (IP address)	IN (0x0001)
May 12, 2021 20:55:38.578542948 CEST	192.168.2.3	8.8.8.8	0xad61	Standard query (0)	hebronbilingualsda.org	A (IP address)	IN (0x0001)
May 12, 2021 20:55:39.601068020 CEST	192.168.2.3	8.8.8.8	0x6c41	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 20:55:19.157399893 CEST	8.8.8.8	192.168.2.3	0xc334	No error (0)	encrypt.techomind.com		162.241.115.110	A (IP address)	IN (0x0001)
May 12, 2021 20:55:36.891705036 CEST	8.8.8.8	192.168.2.3	0x978e	No error (0)	encrypt.techomind.com		162.241.115.110	A (IP address)	IN (0x0001)
May 12, 2021 20:55:38.668457031 CEST	8.8.8.8	192.168.2.3	0xad61	No error (0)	hebronbilingualsda.org		198.12.154.178	A (IP address)	IN (0x0001)
May 12, 2021 20:55:39.659343958 CEST	8.8.8.8	192.168.2.3	0x6c41	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- encrypt.techomind.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49712	162.241.115.110	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 20:55:19.333013058 CEST	1079	OUT	GET / 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: encrypt.techomind.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 20:55:19.497272968 CEST	1085	IN	HTTP/1.1 200 OK Date: Wed, 12 May 2021 18:55:18 GMT Server: Apache Last-Modified: Wed, 12 May 2021 17:12:32 GMT Accept-Ranges: bytes Content-Length: 1547 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html Data Raw: 3c 21 64 6f 63 74 79 70 65 20 70 75 62 6c 69 63 20 22 2d 2f 2f 77 61 70 66 6f 72 75 6d 2f 2f 64 74 64 20 77 6d 6c 20 31 2e 32 2f 2f 65 6e 22 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 54 49 54 4c 45 3e 54 65 63 68 6e 6f 4d 69 6e 64 20 53 65 63 75 72 69 74 79 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 0d 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 66 6f 6e 74 2d 73 69 7a 65 3a 20 35 70 78 3b 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 61 72 69 61 6c 3b 20 22 3e 0d 0a 3c 74 61 62 6c 65 20 73 74 79 6c 65 3d 22 77 69 64 74 68 3a 35 30 70 78 3b 20 62 6f 72 64 65 72 2d 63 6f 6c 6c 61 70 73 65 3a 20 63 6f 6c 6c 61 70 73 65 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 22 3e 20 0d 0a 20 20 20 20 3c 74 62 6f 64 79 3e 3c 74 72 3e 3c 74 64 20 73 74 79 6c 65 3d 22 70 61 64 64 69 6e 67 2d 74 6f 70 3a 20 32 30 70 78 3b 22 3e 0d 0a 20 20 20 20 20 20 20 3c 74 61 62 6c 65 20 73 74 79 6c 65 3d 22 70 61 64 64 69 6e 67 2d 74 6f 70 3a 20 31 30 70 78 3b 20 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 20 31 30 70 78 3b 20 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 20 31 30 70 78 3b 20 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 20 32 30 70 78 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 46 46 46 46 46 46 3b 20 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 43 43 43 43 43 43 3b 20 20 63 6f 6c 6f 72 3a 23 30 30 30 30 30 30 3b 20 77 69 64 74 68 3a 20 34 35 30 70 78 3b 22 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 74 62 6f 64 79 3e 3c 74 72 3e 3c 74 64 3e 3c 69 6d 67 20 73 72 63 3d 27 77 69 6c 64 2e 70 6e 67 27 20 62 6f 72 64 65 72 3d 22 30 22 3e 20 3c 2f 74 64 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 74 64 20 61 6c 69 67 6e 3d 22 72 69 67 68 74 22 3e 3c 69 6d 67 20 73 72 63 3d 27 77 61 79 2e 70 6e 67 27 3e 3c 2f 74 64 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 3c 2f 74 72 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 3c 74 72 3e 3c 74 64 20 63 6f 6c 73 70 61 6e 3d 22 32 22 20 73 74 79 6c 65 3d 22 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 70 78 3b 20 70 61 64 64 69 6e 67 2d 74 6f 70 3a 20 33 30 70 78 3b 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 22 3e 20 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 68 65 62 72 6f 6e 62 69 6c 69 6e 67 75 61 6c 73 64 61 2e 6f 72 67 2f 63 6f 6e 74 65 6e 74 2f 22 20 74 61 72 67 65 74 3d e2 80 9c 5f 62 6c 61 6e 6b e2 80 9d 3e 3c 62 75 74 74 6f 6e 3e 43 6c 69 63 6b 20 48 65 72 65 20 74 6f 20 52 65 61 64 20 4d 65 73 73 61 67 65 3c 2f 62 75 74 74 6f 6e 3e 3c 2f 61 3e 0d 0a 20 20 20 20 20 20 20 20 0d 0a 20 20 20 20 20 20 20 20 20 20 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0d 0a 20 20 20 20 20 20 20 20 20 20 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 74 72 3e 3c 74 64 20 63 6f 6c 73 70 61 6e 3d 22 32 22 20 73 74 79 6c 65 3d 22 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 70 78 3b 20 70 61 64 64 69 6e 67 2d 74 6f 70 3a 20 33 30 70 78 3b 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 22 3e 20 20 3c 61 20 68 72 65 66 3d 22 22 20 73 74 79 6c 65 3d 22 66 6f 6e 74 3a 20 31 32 70 78 20 41 72 69 61 Data Ascii: <!doctype public "-//wapforum//dtd wml 1.2//en"><html><head><TITLE>TechnoMind Security</TITLE><META HTTP-EQUIV="content-type" content="text/html; charset=UTF-8"></head><body style="font-size: 5px; font-family: arial; "> <table style="width:50px; border-collapse: collapse; margin-left: auto; margin-right: auto;"> <tbody><tr><td style= "padding-top: 20px;"> <table style="padding-top: 10px; padding-left: 10px; padding-right: 10px; padding-bottom: 20px; background-color:#FFFFFF; border:1px solid #CCCCCC; color:#000000; width: 450px;"> <tbody><tr><td><img src='wild.png' border="0"> </td> <td align="right"><img src='way.png'></td> </tr> <tr><td colsp an="2" style="font-size: 12px; padding-top: 30px; text-align: center;"> <button>Click Here to Read Message</button> <tr><td colspan="2" styl e="font-size: 12px; padding-top: 30px; text-align: center;"> <a href="" style="font: 12px Aria
May 12, 2021 20:55:19.583978891 CEST	1086	OUT	GET /wild.png HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: http://encrypt.techomind.com/ 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: encrypt.techomind.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 20:55:19.748285055 CEST	1091	IN	HTTP/1.1 200 OK Date: Wed, 12 May 2021 18:55:18 GMT Server: Apache Last-Modified: Wed, 12 May 2021 17:11:13 GMT Accept-Ranges: bytes Content-Length: 3808 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: image/png Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 3d 00 00 00 3f 08 02 00 00 00 dc c8 57 b5 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 01 d5 69 54 58 74 58 4d 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00 00 00 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 58 4d 50 20 43 6f 72 65 20 35 2e 34 2e 30 22 3e 0a 20 20 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 0a 20 20 20 20 20 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 78 6d 6c 6e 73 3a 74 69 66 66 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 74 69 66 66 2f 31 2e 30 2f 22 3e 0a 20 20 20 20 20 20 20 20 20 3c 74 69 66 66 3a 43 6f 6d 70 72 65 73 73 69 6f 6e 3e 35 3c 2f 74 69 66 66 3a 43 6f 6d 70 72 65 73 73 69 6f 6e 3e 0a 20 20 20 20 20 20 20 20 20 3c 74 69 66 66 3a 50 68 6f 74 6f 6d 65 74 72 69 63 49 6e 74 65 72 70 72 65 74 61 74 69 6f 6e 3e 32 3c 2f 74 69 66 66 3a 50 68 6f 74 6f 6d 65 74 72 69 63 49 6e 74 65 72 70 72 65 74 61 74 69 6f 6e 3e 0a 20 20 20 20 20 20 20 20 20 3c 74 69 66 66 3a 4f 72 69 65 6e 74 61 74 69 6f 6e 3e 31 3c 2f 74 69 66 66 3a 4f 72 69 65 6e 74 61 74 69 6f 6e 3e 0a 20 20 20 20 20 20 20 3c 2f 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 3e 0a 20 20 20 3c 2f 72 64 66 3a 52 44 46 3e 0a 3c 2f 78 3a 78 6d 70 6d 65 74 61 3e 0a b0 e3 32 dd 00 00 0c b9 49 44 41 54 68 05 d5 5a 7b 6c 1c c5 19 9f 7d dd cb 77 be d8 8e 5f 75 12 12 3b b4 84 90 84 90 34 50 20 81 0a 8a 48 ab f2 12 a0 f2 47 05 ad 94 84 3f 4a 69 2a 55 6d 41 7d d0 87 aa 4a 40 1f 10 a0 e5 99 14 14 44 4b 90 88 c1 0d a4 52 dc 40 04 24 21 02 f3 b0 49 20 89 1d fb fc 20 f1 f9 79 77 bb b7 bb fd cd ce de dc 78 f7 ee e2 2d 12 11 23 7b f6 9b 6f be c7 6f be fd 66 76 76 f6 24 db b6 c9 17 b0 c8 5f 40 cc 14 b2 3a 4b dc 96 65 a5 d3 69 49 92 0c c3 a8 ac 22 cb 34 16 90 e4 b5 28 5f 92 0f 66 2e 97 cb 1b c6 dc fa fa 50 28 24 ca 97 a3 67 8b 3b e3 94 44 22 61 9a 26 b3 c5 13 cc 03 45 6c 32 1a f2 1e 82 37 99 29 0c 75 2c 9d ce 9b e6 c9 93 27 6b 6a 6a 22 91 48 39 b8 9c ef e2 d6 75 bd 72 20 47 47 d3 c3 a3 a7 c6 a7 33 f9 7c 5e d5 68 21 6c 62 38 71 85 39 b9 40 54 c0 cd e1 ba 32 b2 14 56 55 62 59 c0 3d 31 31 01 23 0b 17 2e 1c 4a a5 6a ea ea 4e 0b 5d d5 3f 78 5f fe e3 3d 19 3d 67 98 95 12 40 33 8c a6 89 94 2c 11 cb b6 01 51 56 35 3e 74 91 a0 c9 c1 8a 54 62 ba bb bd 92 3b a9 a4 ac 69 6e da 2c af bf 91 18 3a f2 10 0a a8 e7 36 34 8c 8c 8c d4 d6 d6 56 86 ae e6 46 4f 55 bd f6 4f cd 26 a5 81 14 60 e0 6a e8 a4 04 16 41 20 28 29 4d 92 6c ea 44 d8 99 0f 34 fd 24 09 b9 07 e8 0d 0d 0d c3 43 43 73 6a 6a 62 b1 58 39 9b aa 2d c9 19 9b 64 2b 20 b2 08 71 52 9a 8a 80 96 89 84 21 16 98 e0 31 3e 65 22 8e 02 df 75 a9 38 fc 52 fe a5 30 b1 1d d0 d4 88 6d b3 bb 01 02 a9 d8 d0 d8 88 84 01 bf 1c 74 d5 26 36 ee 10 bd 49 a5 8a ad 93 d0 6d 9b e2 b7 6c 40 6a d8 99 a9 fc 87 ef 4e 6f fd 6b fe bd 1e 79 d5 8a ea df 6c 91 23 51 40 cd a7 fa 32 cf 3e a6 ef 6a 27 48 b4 af 7c 39 79 ef 93 72 38 42 33 58 92 cc 54 df d8 0f 6e 26 99 6c 29 db ce 20 09 d0 d2 30 63 76 d1 39 e3 4c 12 17 7a 53 d3 e0 e0 20 06 14 ab aa f2 ab d3 79 09 cc Data Ascii: PNGIHDR=?WsRGBiTXtXML:com.adobe.xmp<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="XMP Core 5.4.0"> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:tiff="http://ns.adobe.com/tiff/1.0/"> <tiff:Compression>5</tiff:Compression> <tiff:PhotometricInterpretation>2</tiff:PhotometricInterpretation> <tiff:Orientation>1</tiff:Orientation> </rdf:Description> </rdf:RDF> </x:xmpmeta>2IDAThZ{l}w_u;4P HG?Ji*UmA}J@DKR@$!I ywx-#{oofvv$_@:KeiI"4(_f.P($g;D"a&El27)u,'kjj"H9ur GG3|^h! lb8q9@T2VUbY=11#.JjN]?x_==g@3,QV5>tTb;in,:64VFOUO&`jA ()MlD4$CCsjjbX9-d+ qR!1>e"u8R0mt&6Iml@jNokyl#Q @2>j'H|9yr8B3XTn&l) 0cv9LzS y
May 12, 2021 20:55:19.938215017 CEST	1102	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: encrypt.techomind.com Connection: Keep-Alive
May 12, 2021 20:55:20.101005077 CEST	1104	IN	HTTP/1.1 404 Not Found Date: Wed, 12 May 2021 18:55:19 GMT Server: Apache Accept-Ranges: bytes Keep-Alive: timeout=5, max=98 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html Data Raw: 31 0d 0a 0a 0d 0a 31 0d 0a 0a 0d 0a 31 0d 0a 0a 0d 0a 31 35 37 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 0d 0a 33 0d 0a 34 30 34 Data Ascii: 111157<!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>3404

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49711	162.241.115.110	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 20:55:19.585012913 CEST	1087	OUT	GET /way.png HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: http://encrypt.techomind.com/ 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: encrypt.techomind.com Connection: Keep-Alive
May 12, 2021 20:55:19.749896049 CEST	1095	IN	HTTP/1.1 200 OK Date: Wed, 12 May 2021 18:55:18 GMT Server: Apache Last-Modified: Wed, 12 May 2021 17:11:13 GMT Accept-Ranges: bytes Content-Length: 3775 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: image/png Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 5a 00 00 00 44 08 06 00 00 00 01 74 22 e9 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 01 59 69 54 58 74 58 4d 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00 00 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 58 4d 50 20 43 6f 72 65 20 35 2e 34 2e 30 22 3e 0a 20 20 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 0a 20 20 20 20 20 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 78 6d 6c 6e 73 3a 74 69 66 66 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 74 69 66 66 2f 31 2e 30 2f 22 3e 0a 20 20 20 20 20 20 20 20 20 3c 74 69 66 66 3a 4f 72 69 65 6e 74 61 74 69 6f 6e 3e 31 3c 2f 74 69 66 66 3a 4f 72 69 65 6e 74 61 74 69 6f 6e 3e 0a 20 20 20 20 20 20 3c 2f 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 3e 0a 20 20 20 3c 2f 72 64 66 3a 52 44 46 3e 0a 3c 2f 78 3a 78 6d 70 6d 65 74 61 3e 0a 4c c2 27 59 00 00 0d 14 49 44 41 54 78 01 ed 9b 09 78 53 c5 16 80 cf 6d 92 26 e9 9a ee 50 5a 96 b2 96 d2 22 60 d9 1e 9b b4 c8 26 5a 05 57 90 22 8b 22 2e 0f 11 10 64 f1 fb 14 95 ef 3d 40 11 9e f0 40 1e a2 e2 f2 89 82 4f 45 59 ca e2 f6 d0 62 81 52 d6 52 40 68 59 6c d3 85 ee 4d 93 79 73 e6 76 6e 6f d2 36 29 4d d2 14 cc 7c 1f bd 73 67 bb 67 fe 7b ee 99 33 67 02 80 3b b9 09 b8 09 b8 09 b8 09 b8 09 b8 09 b8 09 b8 09 b8 09 b8 09 b4 50 02 82 a3 e4 7a e8 a5 d5 e4 9b 5f 8e 80 56 ad 02 95 42 e9 a8 61 5d 36 8e 20 10 28 2c ae 80 b6 ad 03 e1 cc b6 55 76 73 b2 7b 00 39 89 59 cb 37 93 2d 3b 0f 82 b1 9a c8 8b 6f d9 fc 1d 9d 23 e1 d0 96 65 0e 61 e4 90 41 2c 49 46 8e 79 96 e4 16 16 5b 16 df 52 f7 0f 26 f4 83 0f 5f 9b e5 30 3e 1e f6 ce be c3 bd cf 91 a1 4f be 6a a6 c2 97 77 ae 15 62 3b 45 d8 3b b4 4b fa 7b 7a 2a 61 d1 d4 a4 3a 90 bd 87 4c 31 9b e3 cd 0a 67 37 68 8d 5a 0d bf 66 64 41 f4 83 73 cd 04 49 fd e0 75 61 fc f0 f8 9b 95 c7 a5 ed db b6 0a 86 1b 07 36 09 4b a6 df 2f 69 f2 e3 4b de 25 9a 81 c9 c4 5e 73 68 37 68 4e e6 42 4e 2e 04 27 3e 65 06 7b eb b2 67 85 8a 5f b6 08 5e 5a 4f de ac c5 5e 87 f5 e9 0e 67 bf 5c 29 01 46 41 fb 25 2f 21 9f a7 fc ea 10 99 1d 06 1a a5 29 29 ab 00 7c fb 93 96 ac 35 03 9e 9f b2 51 88 0c 0b 74 88 c0 ce 18 e4 e9 09 09 f0 fd 9a 97 cc 20 87 8f 9c 45 8e 65 5e 72 d8 e3 1c 0a 9a 4b b5 2d 25 15 fa 27 2f 36 83 9d b9 fd 2d 61 48 ef 6e bc 49 8b b8 06 f8 69 01 bf b8 b7 e6 4c 96 20 bf b8 ea 23 66 2a f2 8b 4b 1d 2a a3 53 40 a3 84 47 33 2f 03 2e 94 72 69 77 af 5d 28 cc 1c 9f 00 82 20 cd 4b 5e dd ac 79 74 dd ae 7e bf de 4c 90 31 b3 ff 41 fe b5 6d 8f 53 e4 70 1a 68 94 f6 6a de 0d f0 19 3c 95 bc b0 ea 03 09 f8 db 2f 4e 16 ca 7f 7e 5f 08 d1 f9 3a 65 42 8d 19 14 17 69 4b ff b8 f3 fd 2f 90 7d bf 9d 68 4c f7 26 b5 71 2a 68 94 a8 da 68 84 75 db 52 00 b5 45 2e a1 2b 5c 40 74 dd 5e 7e e2 3e c0 45 5a 2e 8b 6e d8 34 72 f9 7a be bc c8 e1 79 a7 83 e6 12 a3 b6 c4 3c 34 df 0c 76 73 ba 80 ed c2 83 98 eb b6 74 c6 03 12 64 ee ba 55 54 55 73 31 9d 76 6d 36 d0 38 83 ac ec eb 10 94 38 c3 0c 36 77 01 b5 6a e7 b9 80 b8 08 5b c6 2b 06 4e 7d c5 61 ae 5b 63 de 4e b3 82 46 81 4a Data Ascii: PNGIHDRZDt"sRGBYiTXtXML:com.adobe.xmp<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="XMP Core 5.4.0"> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:tiff="http://ns.adobe.com/tiff/1.0/"> <tiff:Orientation>1</tiff:Orientation> </rdf:Description> </rdf:RDF> </x:xmpmeta>L'YIDATxxSm&PZ"`&ZW"".d=@@OEYbRR@hYlMysvno6)M|sgg{3g;Pz_VBa]6 (,Uvs{9Y7-;o#eaA,IFy[R&_ 0>Ojwb;E;K{z*a:L1g7hZfdAsIua6K/iK%^sh7hNBN.'>e{g_^ZO^g\)FA%/!))|5Qt Ee^rK-%'/6-aHnIiL #f*K*S@G3/.riw](K^yt~L1 AmSphj</N~_:eBiK/}hL&q*hhuRE.+\@t^~>EZ.n4rzy<4vstdUTUs1vm6886wj[+N}a[cNFJ

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49719	162.241.115.110	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 20:55:37.073615074 CEST	1185	OUT	GET /favicon.ico HTTP/1.1 User-Agent: AutoIt Host: encrypt.techomind.com
May 12, 2021 20:55:37.233072042 CEST	1188	IN	HTTP/1.1 404 Not Found Date: Wed, 12 May 2021 18:55:36 GMT Server: Apache Accept-Ranges: bytes Transfer-Encoding: chunked Content-Type: text/html Data Raw: 31 0d 0a 0a 0d 0a 31 0d 0a 0a 0d 0a 31 0d 0a 0a 0d 0a 31 35 37 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 0d 0a 33 0d 0a 34 30 34 Data Ascii: 111157<!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <tit le>3404

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49737	162.241.115.110	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 20:55:42.496195078 CEST	1636	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: encrypt.techomind.com Connection: Keep-Alive
May 12, 2021 20:55:42.659604073 CEST	1637	IN	HTTP/1.1 404 Not Found Date: Wed, 12 May 2021 18:55:41 GMT Server: Apache Accept-Ranges: bytes Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html Data Raw: 31 0d 0a 0a 0d 0a 31 0d 0a 0a 0d 0a 31 0d 0a 0a 0d 0a 31 35 37 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 0d 0a 33 0d 0a 34 30 34 Data Ascii: 111157<!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>3404

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
May 12, 2021 20:55:39.046000004 CEST	198.12.154.178	443	192.168.2.3	49722	CN=hebronbilingualsda.org CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sat Mar 13 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sat Jun 12 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 20:55:39.050723076 CEST	198.12.154.178	443	192.168.2.3	49721	CN=hebronbilingualsda.org CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sat Mar 13 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sat Jun 12 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: iexplore.exe PID: 3236 Parent PID: 792

General

Start time:	20:55:16
Start date:	12/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff705ce0000
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	Completion	Count	Source Address	Symbol

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: 5364 Parent PID: 3236

General

Start time:	20:55:17
Start date:	12/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3236 CREDAT:17410 /prefetch:2
Imagebase:	0x230000
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