ID: 345228
Cookbook: browseurl.jbs
Time: 21:04:05
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

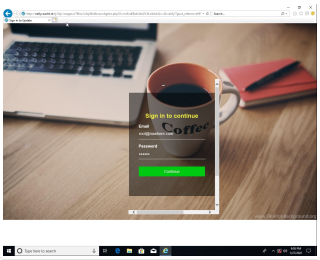
Analysis Report http://nellycoacht.nl/tj/Wp-images/?i=i&…

Overview

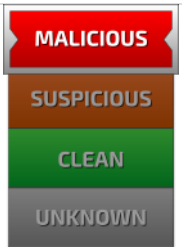
General Information

Sample URL:	http://nellycoacht.nl/tj/Wp-images/?i=i&0=root@nowhere.com
Analysis ID:	345228

Most interesting Screenshot:



Detection



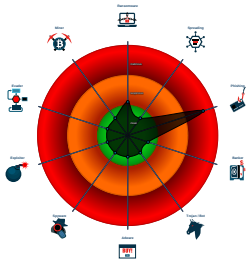
HTMLPhisher

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 HtmlPhish_10
- Yara detected HtmlPhish_16
- Found iframes
- HTML body contains low number of …
- HTML title does not match URL
- None HTTPS page querying sensitiv…
- Suspicious form URL found
- URL contains potential PII (phishing…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 4804 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1852 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4804 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

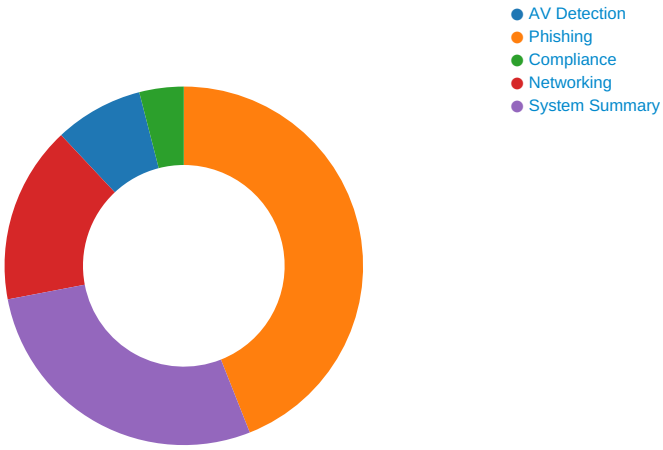
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\src[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\o79foe1v8q20hd8rcawv6gklro[1].htm	JoeSecurity_HtmlPhish_16	Yara detected HtmlPhish_16	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 HtmlPhish_10

Yara detected HtmlPhish_16

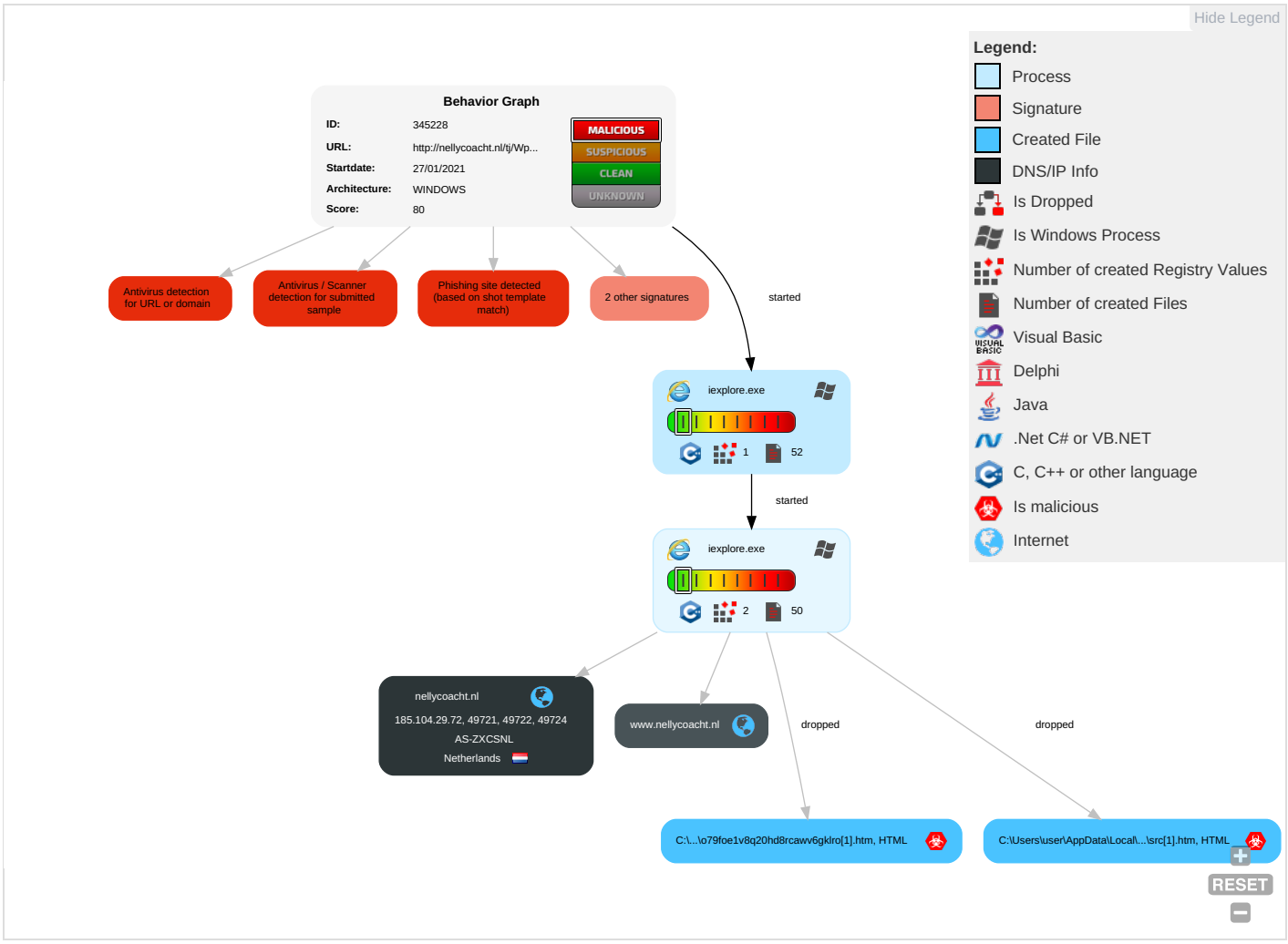
Compliance:

Uses new MSVCR Dlls

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	Non-Application Layer Protocol 3	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	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	Ingress Tool Transfer 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

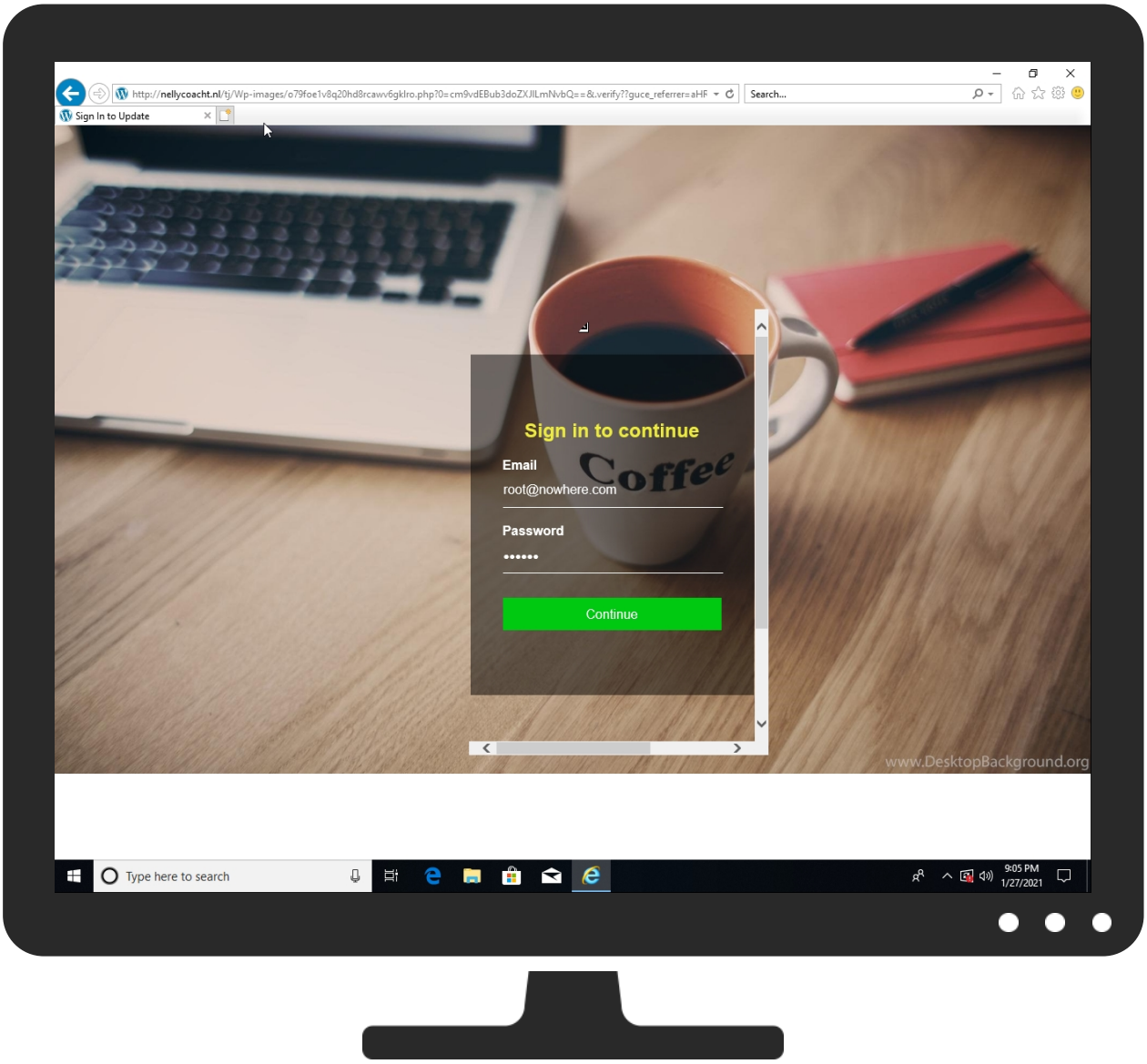
Behavior Graph



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://nellycoacht.nl/tj/Wp-images/?i=i&0=root@nowhere.com	0%	Virustotal		Browse
http://nellycoacht.nl/tj/Wp-images/?i=i&0=root@nowhere.com	100%	Avira URL Cloud	phishing	
http://nellycoacht.nl/tj/Wp-images/?i=i&0=root@nowhere.com	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
www.nellycoacht.nl	0%	Virustotal		Browse
nellycoacht.nl	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://nellycoacht.nl/tj/Wp-images/cache/styles.css	100%	Avira URL Cloud	phishing	
http://nellycoacht.nl/tj/Wp-images/cache/style.css	100%	Avira URL Cloud	phishing	
http://nellycoacht.nl/tj/Wp-images/cache/Technology-Bold.ttf	100%	Avira URL Cloud	phishing	
http://www.nellycoacht.nl/wp-includes/images/w-logo-blue-white-bg.png	100%	Avira URL Cloud	phishing	
http://nellycoacht.nl/tj/Wp-images/o79foe1v8q20hd8rcawv6gklro.php?0=cm9vdEBub3doZXJlLmNvbQ==&.verify	100%	Avira URL Cloud	phishing	
http://nellycoacht.nl/tj/Wp-images/cache/style2.css	100%	Avira URL Cloud	phishing	
http://nellycoacht.nl/tj/Wp-images/cache/background_styles.css	100%	Avira URL Cloud	phishing	
http://nellycoacht.nl/tj/Wp-images/src.php?0=cm9vdEBub3doZXJlLmNvbQ==&a=0	100%	Avira URL Cloud	phishing	
http://nellycoacht.nl/	100%	Avira URL Cloud	phishing	
http://nellycoacht.nl/tj/Wp-images/serv/mode/bg.jpg	100%	Avira URL Cloud	phishing	
http://nellycoacht.nl/tj/Wp-images/cache/bgr.jpg	100%	Avira URL Cloud	phishing	
http://nellycoacht.nl/tj/Wp-images/wnb5nmuvvnokqnrkcr2amw74zt.php?0=cm9vdEBub3doZXJlLmNvbQ==&.verify	100%	Avira URL Cloud	phishing	
http:///favicon.ico	0%	Avira URL Cloud	safe	
http://nellycoacht.nl/tj/Wp-images/cache/script.js	100%	Avira URL Cloud	phishing	
http://nellycoacht.nl/tj/Wp-images/serv/main.ico	100%	Avira URL Cloud	phishing	
http://nellycoacht.nl/favicon.ico	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.nellycoacht.nl	185.104.29.72	true	false	• 0%, Virustotal, Browse	unknown
nellycoacht.nl	185.104.29.72	true	false	• 1%, Virustotal, Browse	unknown

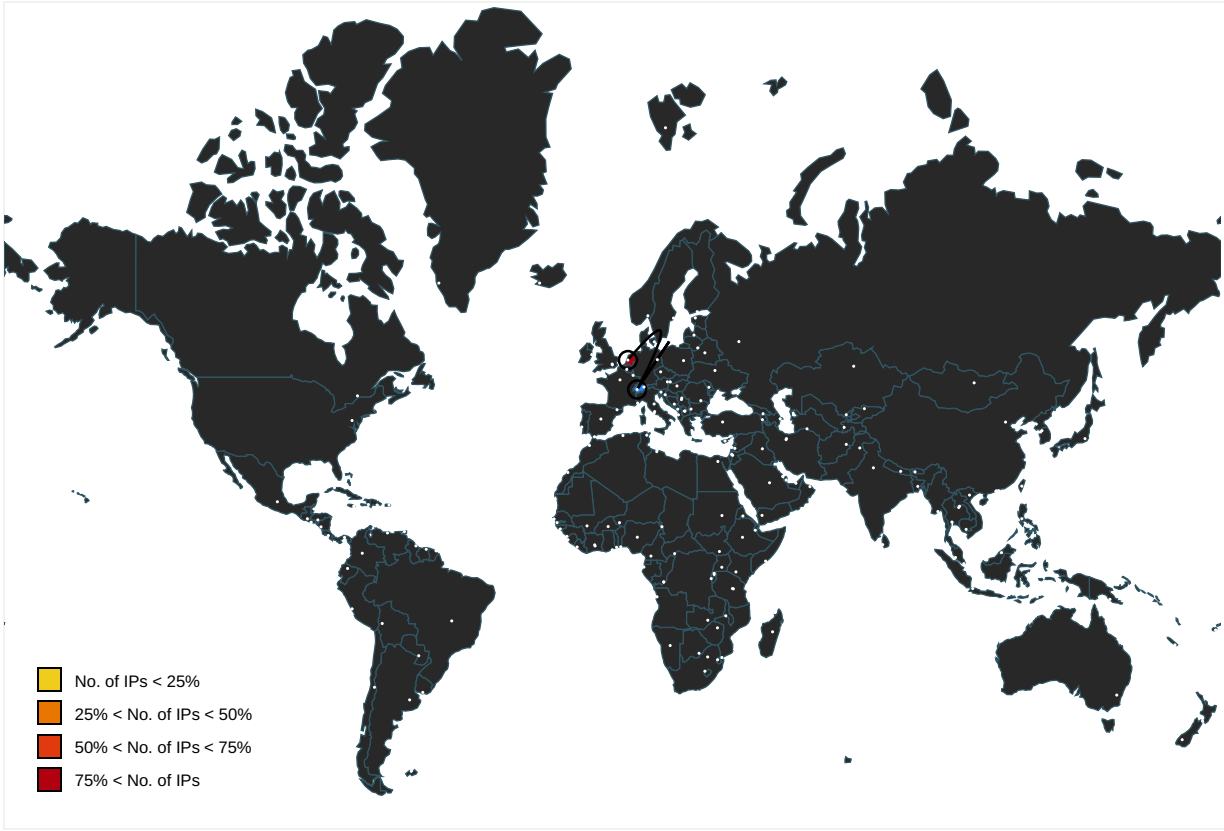
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://nellycoacht.nl/tj/Wp-images/cache/styles.css	true	• Avira URL Cloud: phishing	unknown
http://nellycoacht.nl/tj/Wp-images/?i=i&0=root@nowhere.com	true		unknown
http://nellycoacht.nl/tj/Wp-images/cache/style.css	true	• Avira URL Cloud: phishing	unknown
http://nellycoacht.nl/tj/Wp-images/cache/Technology-Bold.ttf	true	• Avira URL Cloud: phishing	unknown
http://www.nellycoacht.nl/wp-includes/images/w-logo-blue-white-bg.png	true	• Avira URL Cloud: phishing	unknown
http://nellycoacht.nl/tj/Wp-images/cache/style2.css	true	• Avira URL Cloud: phishing	unknown
http://nellycoacht.nl/tj/Wp-images/cache/background_styles.css	true	• Avira URL Cloud: phishing	unknown
http://nellycoacht.nl/tj/Wp-images/src.php?0=cm9vdEBub3doZXJlLmNvbQ==&a=0	true	• Avira URL Cloud: phishing	unknown
http://nellycoacht.nl/tj/Wp-images/serv/mode/bg.jpg	true	• Avira URL Cloud: phishing	unknown
http://nellycoacht.nl/tj/Wp-images/cache/bgr.jpg	true	• Avira URL Cloud: phishing	unknown
http://nellycoacht.nl/tj/Wp-images/cache/script.js	true	• Avira URL Cloud: phishing	unknown
http://nellycoacht.nl/tj/Wp-images/serv/main.ico	true	• Avira URL Cloud: phishing	unknown
http://nellycoacht.nl/favicon.ico	true	• Avira URL Cloud: phishing	unknown

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.2.dr	false		high
http://nellycoacht.nl/tj/Wp-images/o79foe1v8q20hd8rcawv6gklro.php?0=cm9vdEBub3doZXJlLmNvbQ==&.verify	{EA95E8DC-60DA-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: phishing	unknown
http://https://www.coroflot.com/vladimirnikolichttps://www.coroflot.com/vladimirnikolic	Technology-Bold[1].ttf.2.dr	false		high
http://nellycoacht.nl/	{EA95E8DC-60DA-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: phishing	unknown
http://nellycoacht.nl/tj/Wp-images/wnb5nmuvvnokqnrkcr2amw74zt.php?0=cm9vdEBub3doZXJlLmNvbQ==&.verify	{EA95E8DC-60DA-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: phishing	unknown
http:///favicon.ico	src[1].htm.2.dr, o79foe1v8q20hd8rcawv6gklro[1].htm.2.dr	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.104.29.72	unknown	Netherlands		206281	AS-ZXCSNL	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345228
Start date:	27.01.2021
Start time:	21:04:05
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://nellycoacht.nl/tj/Wp-images/?i=i&0=root@nowhere.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:	4
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@3/22@2/1
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, ielowutil.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.108.39.131, 172.217.22.202, 216.58.207.163, 152.199.19.161, 72.247.178.49, 72.247.178.41, 72.247.178.32 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, au.download.windowsupdate.com.edgesuite.net, fonts.googleapis.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus17.cloudapp.net, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.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.{EA95E8DA-60DA-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.852041913712061

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{EA95E8DA-60DA-11EB-90EB-ECF4BBEA1588}.dat	
Encrypted:	false
SSDEEP:	192:r2ZxZe229W8tVifjDuazMWGaBjUaDQsf+DZajX:ryXV2UI6mDhiwovEe
MD5:	C64CD863114BEF62A4DADBCF74BDEC3A
SHA1:	3B212AF39A930E13B0445B9888A6C63BC908C632
SHA-256:	1C0DA15777E3FC239A9D4560B97ED938E177FB7D99CD689AF3F14660D4A8293C
SHA-512:	2C694FB080A37AA6A83A3BB696F8F2D8D11D1FE47A41EC4C5B87734C3179639F72DCA47171B8141DCF5EAB9AA40CDDCEF225097F974DC8E5DAC456FBE979C02
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\{EA95E8DC-60DA-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	46006
Entropy (8bit):	2.6649434600117328
Encrypted:	false
SSDEEP:	384:ruqEwth0yMC0p6we6w8n6wP6w56wi6wNI8V6wPMV6wxa6wN56wx6wn6ws6w3+t66:zjkc5XUZUOBHJKi6
MD5:	8B0D86E92DAE3EE1F9A11CB94676F5D7
SHA1:	89F2BD679B5C139622440E6A533C4F87504462F8
SHA-256:	4F6069B7A106182EBD9769380429EEF633331A572568AC8D72AFB7E6DB878FF6
SHA-512:	2B9DD580E81CBEF8E344ECDFC929AC014151667E9735BE6EF4CB03A3C7BA3CFD7887BAEDE6D0AC62262B62B3CB762991978B57E665E24A7693B46FB6021001D
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\{F1F168EC-60DA-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5673705749790388
Encrypted:	false
SSDEEP:	48:IwXGcpr2GwpaoG4pQQGrapbS9rGQpK7G7HpRgsTGIpG:rdZuQ46uBS9FA6Tg4A
MD5:	C68DA7B30686A9C93B850C552776FE22
SHA1:	6CC21C6B07CFF20F48D2C92503201D924CFFB175
SHA-256:	AA30D32E9507584AB0CA98611D8B0665272049DBCB9CE018B9FFDB83F92DD622
SHA-512:	35CB963BC1C3123E2F57B4A80E4854F17FF64678BD1C17AF73A1A8836C0B126366BD144F2C90564A52CC79B7F2FD26BC343D389915E49F39BB378DD4ADB2E98
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16688
Entropy (8bit):	7.9075053798222905
Encrypted:	false
SSDEEP:	384:WwuxatAVytXnJx4uioDhO7gPCbGST0nb0Nk8XLJ:xBAiqi1KbvJS8bJ
MD5:	8D15925753C2E4518AF08477E3782E65
SHA1:	8D208D5DC13DA8A3B1E2AE1D380C5832CB535ACE
SHA-256:	12C2BF289BAC2988E6D2E1892989FDB45CE2ABA408036C85CBD4E4FF7A72851C
SHA-512:	25DDF106486FE6CB1EF759803D3452CE4FB22BF86AF3DEA4F3F7FE3BD958ECEE227A99E3DCFA81B2513609651C550F38CDC78D824EC727DDD3DA9DA12D98BA9

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Malicious:	false
Reputation:	low
Preview:	0.h.t.t.p.:././.n.e.l.l.y.c.o.a.c.h.t...n.l./.t.j./.W.p.-.i.m.a.g.e.s./.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.....;....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:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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+rtWQguJDXnpikjTzFynVo0GZl9l5Ip4OD7SF6Qvo:pu1xRuq+rsluJNTO1GZzm8FlA
MD5:	14095C75B16E47BCC0F87A3375521A77
SHA1:	38BD291EDA5E6FEC6D2EFBF3CCD258B6986ED69C
SHA-256:	E0820A01E8BE18589121C87E194A0F23F631AD9DA45637C4719D218F5D124BF5
SHA-512:	0BC350D5EDA12152608C8B437EB205BE1E1AAF6EB9A0AE46E7DCD73F82C07A710801C19113DC3CE3D17BCFABA407CABAC8FE21C8DE4B848BC16AD7D3EB71A0D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://nellycoacht.nl/tj/Wp-images/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\2WF3MMUU\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:Qwwg7leQMsCzgeqAaLZKT8FSJiV4e7A8zppGVe2KjfgAUNtWE11OEpXh:gg0QMypZKT8OiV4yA82exjfgAcEQxh
MD5:	C4BC5A8E0C3045A10A8E754E9872187E
SHA1:	6AA1B4A76C73C2660649AFD13B52EE05B27384B3
SHA-256:	BAA0AB5394BD362CABA2A85B0D7C713BA60F58824AEA1B080A2D790752812C01
SHA-512:	0884022641D5E5398DF0786F04D8832FA2884A85B685C7655C066CA38A6B3C9E5A82189F759FE8A225ED2BC40CE743C02B3EDCBA92A5E7ED9230B6D73A12BFEE
Malicious:	false
Reputation:	low
IE Cache URL:	http://nellycoacht.nl/tj/Wp-images/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\2WF3MMUU\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\main[1].ico	
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\2WF3MMUU\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:	78EE99DCA3CAFAAE8A09691C7A4ACB0B9443A6272E96ED0AC4082ACCF91DED40B355B1BF80B4E5DD64A2799458FBC2EC437266BC428B45217DD27ED1A4214 07A
Malicious:	false
Reputation:	low
IE Cache URL:	http://nellycoacht.nl/tj/Wp-images/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..{...ma rgin: 0;...padding: 0;...font-weight: bold;...color: #fff;..}...loginBox input..{...width: 100%;...margin-bottom: 20px;..}...loginBox input[type="text"],...loginBox input[type="pas sword"]..{...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\2WF3MMUU\wnb5nmuvvnokqnrkcr2amw74zt[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	770
Entropy (8bit):	5.466057244291871
Encrypted:	false
SSDEEP:	24:hYeZOzhEmIFM1qc851tFkEVbB2QETqeVP:ENV1qF1tucb3UqeF
MD5:	9386363F2A8FC0DD3802E513AE524A7D
SHA1:	2741D7E99016907B72CBAE59BD42B6EA48766491
SHA-256:	6A68A443BEC1B9243FE86C30B7F6CEC8EF19C75753F8EF68EF7603B54776B709
SHA-512:	C6394F393F497FCD65C9D98CCE13092714AF7C9B29BF9D6FB0A0ACAF6EC36CC71A68F2B023A6C831900F9AAE4D93119C35E1FAD70F17484586D70627DB50F4
Malicious:	false
Reputation:	low
IE Cache URL:	http://nellycoacht.nl/tj/Wp-images/wnb5nmuvvnokqnrkcr2amw74zt.php?0=cm9vdEBub3doZXJlLmNvbQ==&.verify?? guce_referrer=aHR0cHM6Ly9sb2dpbi55YWhvby5jb20v&guce_referrer_sig=AQAAABA99NmGR9iNQOyU5mI3ASjQfYjcPATD_A8modgjxpNXYNmo8n5zxdi8EZV7GFYPz oSc_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">. <li nk 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=cm9vdEBub3doZXJlLmNvbQ==&guce_referrer=aHR0cHM6Ly9sb2dpbi55YWhvby5jb20v&guce_referrer_sig=AQAAABA99NmGR9iNQOyU5mI3A SjQfYjcPATD_A8modgjxpNXYNmo8n5zxdi8EZV7GFYPzoSc_RpMz0hYfdCk0OLmxnMB6tpfZnd5ENc'" />. </head>. <body>. Connecting To Mail Service Provider . . . </body>.</html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\1Ptxg8zYS_SKggPN4iEgvnHyvveLxVvaorCIPrc[1].woff	
IE Cache URL:	http://https://fonts.gstatic.com/s/raleway/v18/1Ptxg8zYS_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.Ru h.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..I: 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\9026IKNJ\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://nellycoacht.nl/tj/Wp-images/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\9026IKNJ\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
Reputation:	low
IE Cache URL:	http://nellycoacht.nl/tj/Wp-images/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\CS6IXJW6\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://nellycoacht.nl/tj/Wp-images/cache/bgr.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\bgr[1].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\CS6IXJW6\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	196
Entropy (8bit):	5.198276883306749
Encrypted:	false
SSDEEP:	6:0IFFUM0+56ZRWHTizlpdOJPL2TDbMJNin:jFuO6ZRoT6pdDb4Y
MD5:	7EB751AF3A277D56358C806A62F63C68
SHA1:	EFDC804F461283E4E7F7C8C4176E08DDDF642261
SHA-256:	65CBF7D1E1D830FDD2EBE7AA9E3827F8E4EBD7D0D800D22105283D39854922B8
SHA-512:	C17AEE6CCBA2AD36C27DA6626C852BAC5B7A8F62F675B013B13F88EBB3BC181D0044F5C71F4206A5DDF17E4AE69351E68BD4A55347303236D7C9A85811912C C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Raleway
Preview:	@font-face {. font-family: 'Raleway';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/raleway/v18/1Ptxg8zYS_SKggPN4iEgvnHyvveLxVvaorCIPr c.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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):	615
Entropy (8bit):	4.978396961374664
Encrypted:	false
SSDEEP:	12:IJtuTjQiBWQicd8wL3vKMlHL3oJDX7L3Wy3la0bvoGu:IJtuP7WJcWaKMCNt36
MD5:	1FA14FADDD68A18E4476B0C7D7A0CB4D
SHA1:	689A84B4E07897367B46C34D1EA23AF5F4AD461D
SHA-256:	3E652405705A2E4773A672C044445C3C67D987B680BCFA95F9DC14CBEE60FFD1
SHA-512:	493A701F90FB81B10C0D1097FE5778BA9FD58FCD411D7116C1C76AB10FE3DD12100EFCDDD0192E97F2C4C2C0C0FA6A16DD5CDC73B64EE687E2FB26BA89C8F CB
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\src[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://nellycoacht.nl/tj/Wp-images/src.php?0=cm9vdEBub3doZXJlLmNvbQ==&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="root@nowhere.com">..... Password .....<input type="password" name="p" required placeholder=".....">..... .....<i nput type="submit" name="" value="Continue">.....</form>.... ...</body>..</html>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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://nellycoacht.nl/tj/Wp-images/cache/background_styles.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\background_styles[1].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\OR0WKIO1\o79foe1v8q20hd8rcawv6gklro[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	492
Entropy (8bit):	5.21176463318556
Encrypted:	false
SSDEEP:	12:YrHw0fKiY+06rXzzKiWvLOZYlPdqSfPRTQL:YrsiY+0uCtvCZafpM
MD5:	1E2FC3C6C68E2D0207970C6BAFAB42B7
SHA1:	3117088AE898745B65C826F48415AC919D7A8B05
SHA-256:	6E2F2E631A7493A1DF9F48EB8CA7542324D063FCA3FE040828CF620C994AFB4D
SHA-512:	CEAD99757FD10F670B0AFB8F9A907FEF14A7B59D03B454EC36F688C38F1ECD529CBB0963EC19B439BF4101F022E0359CD718C8FBA9EF46DAACFDFDF6837783CB
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_16, Description: Yara detected HtmlPhish_16, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\o79foe1v8q20hd8rcawv6gklro[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://nellycoacht.nl/tj/Wp-images/o79foe1v8q20hd8rcawv6gklro.php?0=cm9vdEBub3doZXJlLmNvbQ==&.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=cm9vdEBub3doZXJlLmNvbQ==&a=0" width="370" height="550"></iframe>..</body>.</html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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:dAQnMA9M8lMdMAnGoMGyl60bNhYvr6XXNYBE9RIsjgttt:CQMsRlMdMAX9XHhhYvrEO6zIJbt
MD5:	923D2906F51BE6C3ED49E74EFE7664FF
SHA1:	B1393393B0E96F5C806E6480191E03E10B0D9832
SHA-256:	D6FC3D1520A00BE1C8C8CB060A85BDB76F8DAA6596E58D2B2A977EA67BB0A886
SHA-512:	6B5E755683B32CEC3F9D2E8AE02CCEB6425813304B3C59FF5E5905A2DC7056586AE42D86516193767D079A600B8122D0E90DDB61E2B0747CE8EFA07D201FECD
Malicious:	false
Reputation:	low
IE Cache URL:	http://nellycoacht.nl/tj/Wp-images/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\OR0WKIO1\w-logo-blue-white-bg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 80 x 80, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4119
Entropy (8bit):	7.949120703870044
Encrypted:	false
SSDEEP:	96:h3bdWfcmTY+aRF1pXWZL2+42HGhIUc8KeLEd:hgXTY+as02mOB8XLEd
MD5:	000BF649CC8F6BF27CFB04D1BCDCD3C7
SHA1:	D73D2F6D74EC6CDCBAE07955592962E77D8AE814
SHA-256:	6BDB369337AC2496761C6F063BFFEA0AA6A91D4662279C399071A468251F51F0
SHA-512:	73D2EA5FFC572C1AE73F37F8F0FF25E945AFEE8E077B6EE42CE969E575CDC2D8444F90848EA1CB4D1C9EE4BD725AEE2B4576AFC25F17D7295A90E1CBFE6EDFD5
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.nellycoacht.nl/wp-includes/images/w-logo-blue-white-bg.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\w-logo-blue-white-bg[1].png	
Preview:	.PNG.....IHDR...P...P.....IDATx..].xU...[..V..*).Kk...V.k..J]jKEl?...t...!.{.,...E.....@....F.%.....B...N.y..w.....I{.o...;.s..3...WH...../.zBp.o,XW.....#Z.f...|mvD..9..F.....y..o. ...1^.743l.....v..#.c.E&.e..hU1.{..._cZ..We.v.....f.w....(..6|.Y.. I:x..-.&.....D.....<.6.6.I....T..)...|....#..$g...VN.....!'/6.w..B.h.}....EV.....k.7" f.}.G.~#..M..+....G....iB.....]..?+.. ....'.j.GB..P%.....\...../..%...&.8E..."....44.J...1.....S.....d.j..]ni%._..9.{.O?.H..6T.\|A.GC..g...U.oDEt,?.0....~....q=.y.~.9.Z.....c...v.._....$.0.2...F.9a.L..)..l...2...w...I ..&....Vg.....H.I..r...../....z.`..+...Z.^U.=..5aBpb..0< ../>.9.c...".I..0.3N,}}....|]Fb...Q.....W.....OQ..y;.....|.37..}.....(c.....X..`xX).;.....<5S....>.9..G.:..=..0^.....I_<G.....H....C. O.*.....Hk{..{....]Nc..B.8..}%>..w....Z...).....\..>....c..2...&..0'.DZJ.'~{Y....I....?.....fR.a.....;.<..IRG..n.....Q.....Nf.6.

C:\Users\user\AppData\Local\Temp\~DF1924440C3F6B17B5.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF40FCB4373B29A935.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4757448368911254
Encrypted:	false
SSDEEP:	96:kBqoI3FUd3FUb3FUfUhUl8UwUhU0UfU0U+8UkwUk3:kBqoIm4yIz
MD5:	3D38423F19D16C2103C1DB118C35A5AF
SHA1:	99531F8755B7AEC21DC70932D6A920CA1E2B6666
SHA-256:	43951D643FA1660850E5AEC649F7349F309A49FCF5AB98663EA482B697B8C505
SHA-512:	A384AD6FA3155B72F256890B4A637FBF50A652BC296F413E001B1FD63015CA59C2BE28A9A74140DC60AAB33D9031E12EB5AD5775992396CA20D1037DDE9BECE B
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

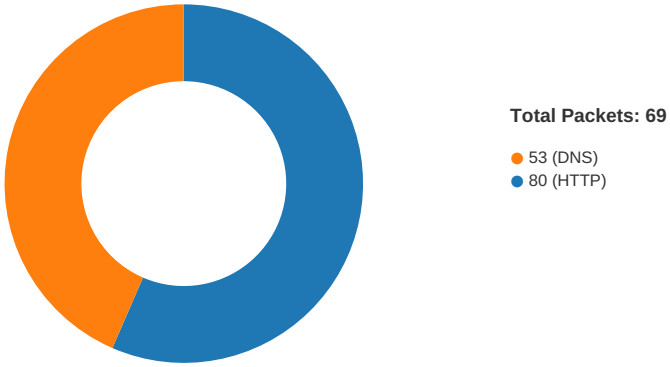
C:\Users\user\AppData\Local\Temp\~DF44BCD26DB75BAA81.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	52240
Entropy (8bit):	1.5792468496078493
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+MqwRaXp6wR6w8n6wP6w56wi6wG06wm6wi6wed66w16wN56wx6wn6e:a7c5XUfQURNBHJKi
MD5:	2504F3D462D4C3278E0ECAB7B565CB15
SHA1:	7079395372C5266966F30B77B74DC7E75BC9073C
SHA-256:	07D08C60AB2504C3CC63A50E30ADE44DD0F3C19DAC4BA91431A5C6ED9E0A8E76
SHA-512:	A60D395BADA769EB69FE2BE50E11830C203F146A6C75284BAA8EDF259247E4E3C0F008C8E5D487D57EE7DF1D5B7B6AF6C738CE6AD51B46CDAD38939596F74F 8F
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
Jan 27, 2021 21:04:55.238400936 CET	49721	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.238486052 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.286083937 CET	80	49721	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.286125898 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.286293030 CET	49721	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.286295891 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.292447090 CET	49721	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.380852938 CET	80	49721	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.439660072 CET	80	49721	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.439810991 CET	49721	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.444240093 CET	49721	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.493915081 CET	80	49721	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.502228975 CET	80	49721	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.502325058 CET	49721	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.579178095 CET	49721	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.581090927 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.584389925 CET	49724	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.631891012 CET	80	49721	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.631972075 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.631999016 CET	49721	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.632076979 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.633493900 CET	49721	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.634042025 CET	80	49724	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.634152889 CET	49724	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.673053980 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.683866978 CET	80	49721	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.684006929 CET	49721	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.734230042 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.734257936 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.734270096 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.734283924 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.734299898 CET	80	49722	185.104.29.72	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 21:04:55.734313965 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.734330893 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.734347105 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.734345913 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.734364986 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.734384060 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.734400034 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.734436035 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.734541893 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.782329082 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.782356977 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.782378912 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.782397985 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.782488108 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.782506943 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.782524109 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.782553911 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.782567978 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.782602072 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.782624960 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.782644033 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.782660961 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.782664061 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.782677889 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.782756090 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.832561970 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.832590103 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.832606077 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.832624912 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.832642078 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.832659006 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.832674980 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.832690954 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.832705975 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.832720041 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.832735062 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.832741022 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.832755089 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.832772017 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.832787991 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.832807064 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.832811117 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.832823992 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.832851887 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.832876921 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.880811930 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.880851984 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.880897045 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.880933046 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.880945921 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.880985022 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.880995035 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.880999088 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.881016016 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.881037951 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.881047964 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.881094933 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.881099939 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.881130934 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.881145000 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.881166935 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.881175995 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.881202936 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.881217003 CET	49722	80	192.168.2.4	185.104.29.72

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 21:04:55.881237030 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.881246090 CET	49722	80	192.168.2.4	185.104.29.72
Jan 27, 2021 21:04:55.881273031 CET	80	49722	185.104.29.72	192.168.2.4
Jan 27, 2021 21:04:55.881278992 CET	49722	80	192.168.2.4	185.104.29.72

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 21:04:50.477365017 CET	57458	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:04:50.534610033 CET	53	57458	8.8.8.8	192.168.2.4
Jan 27, 2021 21:04:51.445972919 CET	50579	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:04:51.498050928 CET	53	50579	8.8.8.8	192.168.2.4
Jan 27, 2021 21:04:52.743899107 CET	51703	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:04:52.791898966 CET	53	51703	8.8.8.8	192.168.2.4
Jan 27, 2021 21:04:53.529001951 CET	65248	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:04:53.577100039 CET	53	65248	8.8.8.8	192.168.2.4
Jan 27, 2021 21:04:54.073746920 CET	53723	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:04:54.133754015 CET	53	53723	8.8.8.8	192.168.2.4
Jan 27, 2021 21:04:54.381177902 CET	64646	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:04:54.429169893 CET	53	64646	8.8.8.8	192.168.2.4
Jan 27, 2021 21:04:55.153947115 CET	65298	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:04:55.223512888 CET	53	65298	8.8.8.8	192.168.2.4
Jan 27, 2021 21:04:55.476963043 CET	59123	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:04:55.526397943 CET	53	59123	8.8.8.8	192.168.2.4
Jan 27, 2021 21:04:55.666603088 CET	54531	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:04:55.734399080 CET	53	54531	8.8.8.8	192.168.2.4
Jan 27, 2021 21:04:55.962372065 CET	49714	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:04:56.022295952 CET	53	49714	8.8.8.8	192.168.2.4
Jan 27, 2021 21:04:56.990809917 CET	58028	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:04:57.039241076 CET	53	58028	8.8.8.8	192.168.2.4
Jan 27, 2021 21:04:58.156162977 CET	53097	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:04:58.205830097 CET	53	53097	8.8.8.8	192.168.2.4
Jan 27, 2021 21:04:59.023533106 CET	49257	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:04:59.074273109 CET	53	49257	8.8.8.8	192.168.2.4
Jan 27, 2021 21:04:59.882205009 CET	62389	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:04:59.932982922 CET	53	62389	8.8.8.8	192.168.2.4
Jan 27, 2021 21:05:00.784854889 CET	49910	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:05:00.834768057 CET	53	49910	8.8.8.8	192.168.2.4
Jan 27, 2021 21:05:01.136025906 CET	55854	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:05:01.198843002 CET	53	55854	8.8.8.8	192.168.2.4
Jan 27, 2021 21:05:01.613986015 CET	64549	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:05:01.661890984 CET	53	64549	8.8.8.8	192.168.2.4
Jan 27, 2021 21:05:02.480333090 CET	63153	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:05:02.528179884 CET	53	63153	8.8.8.8	192.168.2.4
Jan 27, 2021 21:05:03.656361103 CET	52991	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:05:03.704291105 CET	53	52991	8.8.8.8	192.168.2.4
Jan 27, 2021 21:05:24.065854073 CET	53700	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:05:24.118083000 CET	53	53700	8.8.8.8	192.168.2.4
Jan 27, 2021 21:05:24.763787031 CET	51726	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:05:24.815207005 CET	53	51726	8.8.8.8	192.168.2.4
Jan 27, 2021 21:05:25.366468906 CET	53700	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:05:25.418418884 CET	53	53700	8.8.8.8	192.168.2.4
Jan 27, 2021 21:05:25.770100117 CET	51726	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:05:25.820029974 CET	53	51726	8.8.8.8	192.168.2.4
Jan 27, 2021 21:05:26.379414082 CET	53700	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:05:26.427229881 CET	53	53700	8.8.8.8	192.168.2.4
Jan 27, 2021 21:05:26.785825014 CET	51726	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:05:26.833712101 CET	53	51726	8.8.8.8	192.168.2.4
Jan 27, 2021 21:05:28.380229950 CET	53700	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:05:28.428302050 CET	53	53700	8.8.8.8	192.168.2.4
Jan 27, 2021 21:05:28.801503897 CET	51726	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:05:28.850215912 CET	53	51726	8.8.8.8	192.168.2.4
Jan 27, 2021 21:05:32.395524025 CET	53700	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:05:32.445563078 CET	53	53700	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 21:05:32.802076101 CET	51726	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:05:32.849832058 CET	53	51726	8.8.8.8	192.168.2.4
Jan 27, 2021 21:05:38.589724064 CET	56794	53	192.168.2.4	8.8.8.8
Jan 27, 2021 21:05:38.647510052 CET	53	56794	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 21:04:55.153947115 CET	192.168.2.4	8.8.8.8	0x3d93	Standard query (0)	nellycoacht.nl	A (IP address)	IN (0x0001)
Jan 27, 2021 21:05:01.136025906 CET	192.168.2.4	8.8.8.8	0x90d8	Standard query (0)	www.nellycoacht.nl	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 21:04:55.223512888 CET	8.8.8.8	192.168.2.4	0x3d93	No error (0)	nellycoacht.nl		185.104.29.72	A (IP address)	IN (0x0001)
Jan 27, 2021 21:05:01.198843002 CET	8.8.8.8	192.168.2.4	0x90d8	No error (0)	www.nellycoacht.nl		185.104.29.72	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- nellycoacht.nl
- www.nellycoacht.nl

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49721	185.104.29.72	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 21:04:55.292447090 CET	62	OUT	GET /tj/Wp-images/?i=i&0=root@nowhere.com 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: nellycoacht.nl Connection: Keep-Alive
Jan 27, 2021 21:04:55.439660072 CET	62	IN	HTTP/1.1 302 Moved Temporarily date: Wed, 27 Jan 2021 20:04:55 GMT server: Apache/2 x-powered-by: PHP/7.0.33 expires: Thu, 19 Nov 1981 08:52:00 GMT cache-control: no-store, no-cache, must-revalidate pragma: no-cache set-cookie: PHPSESSID=53nuvstp9nkf8a2560pn9snkm3; path=/ upgrade: h2,h2c connection: Upgrade location: wnb5nmuvvnokqnrkcr2amw74zt.php?0=cm9vdEBub3doZXJlLmNvbQ==&.verify??guce_referrer=aHR0cHM6Ly9sb2dpbi55YWhvby5jb20v&guce_referrer_sig=AQAAABA99NmGR9iNQOyU5mI3ASjQfYjcPATD_A8modgjxpNXYNmo8n5zxdi8EZV7GFYPzoSc_RpMz0hYfdCk0OLmxnMB6tpfZnd5ENcxTcI3e56K0Vz3pSL6PoIoDveE6VV6vAiBzqdjcYAbAHdiaf7gx2w9XRGmCh4orbe2VcZO9aN_ vary: User-Agent content-length: 0 content-type: text/html; charset=UTF-8
Jan 27, 2021 21:04:55.444240093 CET	63	OUT	GET /tj/Wp-images/wnb5nmuvvnokqnrkcr2amw74zt.php?0=cm9vdEBub3doZXJlLmNvbQ==&.verify??guce_referrer=aHR0cHM6Ly9sb2dpbi55YWhvby5jb20v&guce_referrer_sig=AQAAABA99NmGR9iNQOyU5mI3ASjQfYjcPATD_A8modgjxpNXYNmo8n5zxdi8EZV7GFYPzoSc_RpMz0hYfdCk0OLmxnMB6tpfZnd5ENcxTcI3e56K0Vz3pSL6PoIoDveE6VV6vAiBzqdjcYAbAHdiaf7gx2w9XRGmCh4orbe2VcZO9aN_ 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: nellycoacht.nl Connection: Keep-Alive Cookie: PHPSESSID=53nuvstp9nkf8a2560pn9snkm3

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 21:04:55.502228975 CET	64	IN	HTTP/1.1 200 OK date: Wed, 27 Jan 2021 20:04:55 GMT server: Apache/2 x-powered-by: PHP/7.0.33 upgrade: h2,h2c connection: Upgrade vary: Accept-Encoding,User-Agent content-encoding: gzip content-length: 514 content-type: text/html; charset=UTF-8 Data Raw: 1f 8b 08 00 00 00 00 00 00 03 8d 52 4d 73 9b 30 14 3c d7 bf 42 d5 a1 39 19 68 52 52 bb 45 ee e0 8f 26 ed f8 db 4e 1b 7c f1 08 49 06 39 20 51 49 a6 c6 bf be c2 38 e9 64 7a e9 01 d0 88 dd f7 f6 ed be e0 ed 70 36 58 47 f3 11 48 4d 9e f5 5a 41 f3 01 20 48 19 a6 e7 43 c6 c5 13 50 2c 43 50 a7 52 19 72 30 80 13 29 20 30 55 c1 10 e4 39 4e 98 5b 88 04 82 54 b1 9d 45 31 55 ba 39 e6 c2 b1 30 e8 d6 35 5e 57 31 55 c6 74 ca 98 79 66 10 4c 52 e6 c6 98 3c 25 4a 1e 04 dd 36 10 87 68 0d ff 9b fe 2f 47 13 c5 0b 03 b4 22 2f 98 f3 8d b3 d7 10 50 b6 63 aa 17 5c ae 2e 0c c3 4d c6 7a 43 66 18 31 5c 24 60 82 79 06 56 76 1e a6 1c c7 09 dc e6 7f eb 4d 90 33 83 ad 63 a6 68 b3 5f 07 5e 22 68 85 28 ab 0a 02 eb 8c 61 c2 20 f8 e1 33 78 58 8e d1 55 26 31 75 8a b4 f8 e2 21 92 77 4b 3a ea 1f e2 1b 2a 37 8f df b3 71 3e 2d e3 05 42 ef 92 03 61 5b 55 2b 52 4c 21 7c bf f4 c8 fd e4 76 5c 75 75 7c 4d 8b 98 fb 7e f4 33 2d e3 ca df c7 d7 5e f9 1a be d5 3c 41 e1 22 0c c3 7e d8 ed 4e f3 bb 65 97 4f 17 b3 ea c1 cf bf dd 84 ab fd 62 17 ed c9 3c 5c 0f b7 61 27 97 34 d9 1f 8b e9 63 34 cd 65 47 f8 a7 23 e5 9d d1 e6 c7 c7 bb af d1 fc 24 57 64 bb 2c 26 27 2f 8d 76 74 f0 e4 cd c6 f9 51 4c fa b7 a6 d8 6d 04 f5 47 53 72 05 c1 39 cf c0 7d d9 8e 58 d2 ca 1e 02 62 87 ae 0d a5 bc 04 9c 5a c3 a5 10 b0 37 b0 ef 8b 97 6b f9 d7 4e 4e 18 98 2b 59 72 ca 54 e0 5a 8a 0d e2 b9 40 dc 3c 2d d0 44 52 d7 23 19 d6 1a c1 42 c9 c4 9a ac db 31 56 10 9c f3 46 b0 dd fe cd a9 49 3f 81 f7 9e 0d 15 1b dc ce 70 5c ef 49 dd fa d2 db 66 07 7b 4d 9f b3 f8 46 b3 1d a2 de f5 3f e9 c2 ca d0 02 03 00 00 Data Ascii: RMs0<B9hRRE&N|I9 QI8dzp6XGHMZA HCP,CPRr0) 0U9N[TE1U905^W1UtyfLR<%J6h/G"/Pc\.MzCf1\$`yVvM 3ch_^"h(a 3xXU&1u!wK:*7q>-Ba[U+RL!|v\uu|M~3-^<A"~NeOb<\a'4c4eG#$Wd,&'/vtQLmGSr9}XbZ7kNN+YrTZ@<-DR#B1 VFI?p\lf{MF?
Jan 27, 2021 21:04:55.579178095 CET	65	OUT	GET /tj/Wp-images/cache/background_styles.css HTTP/1.1 Accept: text/css, */* Referer: http://nellycoacht.nl/tj/Wp-images/wnb5nmuvvnokqnrkcr2amw74zt.php?0=cm9vdEBub3doZXJlLmNvbQ==&.verify??guce_referrer=aHR0cHM6Ly9sb2dpbi55YWhvby5jb20v&guce_referrer_sig=AQAAABA99NmGR9iNQOyU5mI3ASjQfYjcPATD_A8modgjxpNXYNmo8n5zxdi8EZV7GFYPzoSc_RpMz0hYfdCk0OLmxnMB6tpfZnd5ENcxTcI3e56K0Vz3pSL6PoIoDveE6VV6vAiBzqdjcYAbAHdiaf7gx2w9XRGmCh4orbe2VcZO9aN_ 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: nellycoacht.nl Connection: Keep-Alive Cookie: PHPSESSID=53nuvstp9nkf8a2560pn9snkm3
Jan 27, 2021 21:04:55.631891012 CET	67	IN	HTTP/1.1 200 OK date: Wed, 27 Jan 2021 20:04:55 GMT server: Apache/2 upgrade: h2,h2c connection: Upgrade last-modified: Tue, 26 Jan 2021 21:52:26 GMT etag: "1d8-5b9d4ab9b13d1-gzip" accept-ranges: bytes vary: Accept-Encoding,User-Agent content-encoding: gzip content-length: 293 content-type: text/css Data Raw: 1f 8b 08 00 00 00 00 00 00 03 6d 50 db 4a 03 31 14 7c de 7c 45 a0 48 ad b0 17 a9 50 d8 45 2c a2 7e 80 f8 03 69 36 b7 9a 6c 42 92 75 5d 4b ff dd b3 97 62 5b 24 10 c8 cc 64 e6 cc d9 2a e3 ac 8f b8 f5 fa 76 29 63 74 a1 cc 73 6e 9b 18 32 61 ad d0 8c 38 15 32 6a 4d 4e 43 78 e2 c4 28 dd 3f be 13 cd 3a d2 2f 57 15 da 0e da 94 13 ca f0 01 61 3c bf 06 55 89 3f 18 95 8d d5 56 f4 15 4a 82 a7 e5 98 f2 87 a6 cf 56 d7 59 8c 1c 7c 92 23 42 77 a3 c5 95 c9 9c 55 21 10 c8 68 f4 ac e9 54 1d 65 89 ef 8b e2 a6 1a 01 c9 94 90 f1 1c a9 55 70 9a 80 05 d7 ec 7b 82 f6 6d 88 8a f7 29 85 04 d6 80 9a c2 cd fc 44 12 ad 44 93 aa c8 4c b8 24 76 84 7e 0a 6f db a6 86 8f da fa 12 2f 5e de 86 03 63 9f 71 ca 10 c1 a6 8e 3b e1 b3 bd 13 ab 4b 41 50 3f c0 53 fb 35 18 27 43 a1 05 0c d2 a0 03 4a c6 ca 13 bf 2e 1c 4c 3b 21 dd 5c 6a 07 8b 02 ec 94 5e ac 37 af 9b 87 93 e8 bf 75 1f 7f 01 63 ce 6b e6 d8 01 00 00 Data Ascii: mPJ1||EHPE,~i6lBu]Kb[$d*v)ctsn2a82jMNCx(?:/Wa<U?VJVY\|#BwU!hTeUp{m)DDL$v~o/^cq;KAP?S5'CJ. L;!\j^7uck
Jan 27, 2021 21:04:55.633493900 CET	68	OUT	GET /tj/Wp-images/cache/script.js HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: http://nellycoacht.nl/tj/Wp-images/wnb5nmuvvnokqnrkcr2amw74zt.php?0=cm9vdEBub3doZXJlLmNvbQ==&.verify??guce_referrer=aHR0cHM6Ly9sb2dpbi55YWhvby5jb20v&guce_referrer_sig=AQAAABA99NmGR9iNQOyU5mI3ASjQfYjcPATD_A8modgjxpNXYNmo8n5zxdi8EZV7GFYPzoSc_RpMz0hYfdCk0OLmxnMB6tpfZnd5ENcxTcI3e56K0Vz3pSL6PoIoDveE6VV6vAiBzqdjcYAbAHdiaf7gx2w9XRGmCh4orbe2VcZO9aN_ 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: nellycoacht.nl Connection: Keep-Alive Cookie: PHPSESSID=53nuvstp9nkf8a2560pn9snkm3

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 21:04:55.683866978 CET	70	IN	HTTP/1.1 200 OK date: Wed, 27 Jan 2021 20:04:55 GMT server: Apache/2 upgrade: h2,h2c connection: Upgrade last-modified: Tue, 26 Jan 2021 21:52:26 GMT etag: "118-5b9d4ab9b13d1-gzip" accept-ranges: bytes vary: Accept-Encoding,User-Agent content-encoding: gzip content-length: 197 content-type: application/javascript Data Raw: 1f 8b 08 00 00 00 00 00 00 03 55 8e 41 0b 82 40 10 85 ef fe 8a b9 b9 4b 2a 76 e8 68 87 a4 a0 4b 04 41 97 e8 b0 e9 60 c1 ea ca ce 58 48 f6 df 5b a5 d2 6e c3 f0 be ef bd cc 54 c4 50 5b 53 58 24 5a 29 0b 09 e4 26 6b 4a ac 38 2a 90 d7 1a fb 93 56 6d aa 15 d1 4e 95 28 fc 6f 3c bc 28 eb cb 53 7c f6 08 79 5b 31 da bb d2 42 48 48 96 f0 f4 00 b2 41 9e 99 b2 6e 18 f3 03 b7 1a 9d de 59 d3 e9 4b 4c da e5 8f 7a dc 72 be ba 74 ad 2c e1 46 1b c5 e2 4f d4 8f db 5b 53 a3 e5 f6 a8 74 e3 66 85 e1 00 f9 52 42 d7 41 ec 54 13 73 44 03 45 23 35 02 c1 a7 6d 06 d1 5c 7a af 00 16 f2 0d 46 57 57 ac 18 01 00 00 Data Ascii: UA@K*vhKA`XH[nTP[SX$Z)&kJ8*VmN(o<(S|y[1BHHAnYKLzrt,FO[StfRBATsDE#5m\zFWW
Jan 27, 2021 21:04:55.972803116 CET	230	OUT	GET /tj/Wp-images/cache/Technology-Bold.ttf HTTP/1.1 Accept: */* Referer: http://nellycoacht.nl/tj/Wp-images/wnb5nmuvvnokqnrkcr2amw74zt.php?0=cm9vdEBub3doZXJlLmNvbQ==&.verify??guce_referrer=aHR0cHM6Ly9sb2dpbi55YWhvby5jb20v&guce_referrer_sig=AQAAABA99NmGR9iNQOyU5ml3ASjQfYjcPATD_A8modgjxpNXYNmo8n5zxdi8EZV7GFYPzoSc_RpMz0hYfdCk0OLmxnMB6tpfZnd5ENcxTcI3e56K0Vz3pSL6PoIoDveE6VV6vAiBzqdjcYAbAHdiaf7gx2w9XRGmCh4orbe2VcZO9aN_ Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Origin: http://nellycoacht.nl Accept-Encoding: gzip, deflate Host: nellycoacht.nl Connection: Keep-Alive Cookie: PHPSESSID=53nuvstp9nkf8a2560pn9snkm3
Jan 27, 2021 21:04:56.026969910 CET	348	IN	HTTP/1.1 200 OK date: Wed, 27 Jan 2021 20:04:56 GMT server: Apache/2 upgrade: h2,h2c connection: Upgrade last-modified: Tue, 26 Jan 2021 21:52:26 GMT etag: "a1b0-5b9d4ab9b13d1-gzip" accept-ranges: bytes vary: Accept-Encoding,User-Agent content-encoding: gzip access-control-allow-origin: * content-length: 14294 content-type: application/x-font-ttf Data Raw: 1f 8b 08 00 00 00 00 00 00 03 ed 7d 09 80 5c 55 95 f6 79 4b d5 ab de ab bb aa 7a 4d 77 57 6f 69 92 4e ba d3 e9 a4 3b 49 67 23 6b 77 f6 8d 90 06 02 09 49 48 02 d9 4c 02 09 ab 71 03 8c 82 3a 28 b2 44 c4 05 5c c6 25 28 09 09 81 01 19 47 64 11 5a 04 47 67 30 22 bf 33 3a 32 a0 a2 8c 8e 9a ea ff 3b 77 79 ef 56 55 77 16 70 d4 f9 7f 2a e9 73 cf bb f7 be fb de bb ef 9c 73 cf 39 f7 9e fb c8 22 a2 28 80 4b b4 60 c5 f2 9e 3f f6 e4 6e 21 72 86 21 77 e9 e2 e5 6d 63 d7 7d f3 82 d9 44 d6 8d 38 5e b3 72 d6 c2 55 db 4a 2f 7f 00 e5 3b 88 42 2f ad db ba 76 47 f4 e3 65 51 34 70 23 9f b3 ee 8a dd 49 ba 2c 74 98 28 b1 09 f5 4b 2f d9 b1 71 6b b8 ef 40 17 51 ec b3 68 63 d7 c6 2d 57 5e 72 7c e7 57 d6 a3 7c 1f d1 fb 22 9b d6 6f dd fb d4 c3 07 5b 89 72 96 10 79 13 36 6d 58 bb be 38 72 cb 7d a8 9b 8f f3 3b 37 21 c3 5d 44 fd 38 9e 85 e3 c6 4d 5b 77 ef bd fc 65 ef a7 38 fe 39 fe c6 6d d9 be 6e ed 4b 45 6e 23 d1 1d 7c 7f 07 b6 ae dd bb c3 5e 6b 7f 05 65 7c fd e4 b6 b5 5b 37 6c 58 f3 c8 0d 44 77 a2 4e e8 f1 1d db 77 ed 5e f5 b5 0b 8e 13 dd fd 9f 28 ff c6 8e 9d 1b 76 3c 3d e5 da 42 dc 4f 39 8e 17 11 f7 05 fe 96 fd 3c b7 f4 a2 a2 c9 6f 50 85 83 eb 10 fd 60 ea cd 07 64 fa 8d 6b 07 6e 1a b8 d5 ea 47 ff 58 94 43 36 c9 1f ce b1 5f 1b 08 03 79 1d e5 fb ad 7e d1 92 f9 5b 28 72 16 d2 7e 9c a5 ce c0 2f 17 e7 91 dd 20 70 c7 ba c9 7e 88 42 e4 da 0f d9 fb 71 fc 41 99 5a 3f a2 b1 f4 87 8c d6 d2 5a 5f d2 b7 6c 39 25 81 5c 25 ef 01 f7 76 a9 ae 63 fd 16 6d 12 97 5a 8f a8 53 91 5a 78 03 d6 01 4a 5a 1f a5 5a 1c d7 e1 af 9e 3e 42 55 0a af b3 5e a7 6a ce b3 6e 43 1d 3e 3e 24 d2 06 91 f7 08 ce f9 3a e5 8a f4 01 fc bd 4e 35 d6 dd 54 8e e3 1a eb 5e 2a 46 9a 54 7f 75 d6 c7 14 7e 00 f8 50 d7 ba 4d 5c af 46 b5 3d d8 b5 f2 8c 6b d5 9a d7 32 da a9 c5 35 a2 d6 fd aa 4c e6 d5 20 af 40 97 d3 ed 48 ef c2 fd e5 51 11 dd 4d 4d 74 17 d5 e0 af ce 72 a8 12 c7 8d 74 2b 7a e9 ee 81 9b cc fb e6 37 66 89 df 02 fe 95 2e 40 da b1 80 21 fe 14 94 45 56 cb 02 5d d4 22 8b 66 2d 50 e5 5d 7c fe f0 59 5d 6d 38 d2 6f 4f b4 49 f9 f4 fb c8 00 45 c8 1b 18 00 55 44 00 73 01 53 94 47 39 80 f9 94 0b 58 40 79 80 85 94 0f 58 24 60 94 0a 00 8b a9 10 b0 84 8a 00 63 14 1d 38 41 71 01 13 54 0c 58 4a 25 80 65 14 03 2c a7 38 60 85 80 95 94 00 ac a2 52 c0 61 54 06 58 4d e5 03 7f 42 4f 30 ac a5 0a c0 24 55 02 d6 51 15 60 3d 0d 03 6c 10 b0 91 aa 01 9b a8 06 70 38 d5 0e fc 91 9a 29 09 78 96 80 23 a8 0e 70 24 d5 03 b6 50 03 e0 28 6a 04 1c 2d 60 2b 35 01 b6 d1 70 c0 31 d4 3c f0 07 6a a7 b3 00 c7 0a d8 41 23 00 c7 d1 48 c0 f1 d4 02 d8 29 60 17 8d 02 9c 40 a3 01 27 52 eb c0 7f d3 24 6a 03 ec 16 70 32 8d 01 9c 42 ed 80 53 69 2c e0 34 ea 00 9c 2e e0 d9 34 0e 70 06 8d 07 9c 49 9d 03 bf a7 59 d4 05 38 5b c0 39 34 01 70 2e 4d 04 ec a1 49 80 bd d4 0d 38 4f c0 f9 34 19 70 01 4d 19 f8 1d 38 76 2a e0 22 9a 06 b8 58 c0 25 34 1d 70 29 9d 0d b8 8c 66 00 2e a7 99 80 2b 04 3c 87 66 0d fc 17 ad a4 d9 80 e7 d2 1c c0 55 34 17 b0 4f c0 f3 a8 07 f0 7c ea 05 bc 80 e6 01 ae a6 f9 80 17 0a 78 11 Data Ascii: }\UyKzMwWoiN;Ig#kwIHLq:(D\%(GdZGg0"3:2;wyVUwp*ss9"(K`?n!r!wmc}D8^rUJ/;B/vGeQ4p#I,t(K/qk@Qhc-W^r|W|"o[ry6mX8r};7!]D8M[we89mnKEn#|^ke|[7lXDwNw^(v<=BO9<oP`dknGXC6_y~[(r~/ p~BqAZ?Z_l9%\%vcmZSZ xJZZ>BU^jnC>>$:N5T^*FTu~PM\F=k25L @HQMMtrt+z7f.@!EV]"f-P]\|Y]m8oOIEUDsSG9X@yX$`c8AqTXJ%e,8` RaTXMBO0$UQ`=lp8)x#p$P(j-`+5p1<jA#H)`@'R$jp2BSi,4.4pIY8[94p.MI8O4pM8v*"X%4p)f.+<fU4O|x
Jan 27, 2021 21:04:56.394076109 CET	411	OUT	GET /tj/Wp-images/serv/main.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: nellycoacht.nl Connection: Keep-Alive Cookie: PHPSESSID=53nuvstp9nkf8a2560pn9snkm3

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 21:04:56.445745945 CET	413	IN	HTTP/1.1 200 OK date: Wed, 27 Jan 2021 20:04:56 GMT server: Apache/2 upgrade: h2,h2c connection: Upgrade last-modified: Tue, 26 Jan 2021 21:52:26 GMT etag: "302b-5b9d4ab9b42b1-gzip" accept-ranges: bytes vary: Accept-Encoding,User-Agent content-encoding: gzip content-length: 11452 content-type: image/x-icon Data Raw: 1f 8b 08 00 00 00 00 00 00 03 95 7a 05 58 54 5b f4 ef 24 0c 0c 31 43 37 43 3a 20 20 dd dd dd 29 48 49 0b 48 4b 88 0c dd 0d 12 82 d2 21 4a 0a 02 16 2d 2d 2d 21 25 82 94 48 2b 08 f8 06 bd d7 7b ef ff 7d ef 7b ef 9d 33 df 9e 33 fb ac bd f6 fa fd f6 da 6b ed 7d e6 fc 9c fe b9 04 40 a8 2b ab 29 03 80 40 20 c0 1a 7b 02 7e 5e 00 24 14 f4 95 e4 0c 75 f4 c5 51 8e 76 dc 2e 1e f6 8e 28 3f 3e 1e 5e 14 da d7 db d9 dd 11 a5 a6 ae 82 52 d7 55 52 41 f9 09 f3 73 70 a1 3c 7d 6d 5c 9d 7d 02 50 52 28 31 5e fc 9f 73 00 05 00 18 04 ba fc 60 0f 08 f6 03 85 41 a1 10 08 14 1f 17 17 07 46 80 4f 40 00 c7 87 c3 09 89 48 10 84 44 48 22 38 1c 41 81 40 92 92 91 93 93 13 10 53 52 51 90 51 91 90 91 93 5d 2a 01 82 b1 6d 20 50 3c 28 14 8f 8c 10 4e 48 f6 ff 7d fc ec 00 20 61 c0 14 60 0a 18 c8 0c 00 21 81 60 24 f0 67 17 80 0e 8b 13 00 02 63 8b 3f 07 10 8a 03 c6 85 41 40 d8 bb b4 ff db 4d ec 5d 08 0e 2e 18 f4 73 16 40 00 c6 de 44 80 11 d8 ba 23 55 92 50 a8 7c 5b 05 1c 00 45 c1 81 6a f6 6c f2 fd 78 6a 72 64 08 5d 36 36 48 41 46 26 be 3c 06 a4 8b 15 23 43 e9 b2 61 eb d1 20 5d 75 80 3a 20 83 04 c3 86 55 88 f7 fb 77 1c 84 1c 1f 0f db 30 cc 4c 0e fb 0d 00 c8 87 a2 d5 01 99 70 32 14 3a 92 4d b6 08 50 6b 26 fb c7 02 7c d9 f1 67 5c 12 c3 5f f3 81 03 2b 36 8b 26 26 03 6b 5b 62 14 62 d2 66 d4 49 69 7d 75 69 d4 6a 09 d4 ca 9c d4 e6 b1 51 96 b6 1c 59 36 3d 36 51 d4 f7 29 a8 9b 48 14 44 db 3b c5 db 15 24 db 12 0e 40 02 83 04 da 81 87 3b 70 62 bb af 5b 63 b4 5f ab 79 3e 65 f1 27 00 ae e8 7e 39 c7 d3 7b 11 79 45 01 bc b1 c3 90 d9 22 78 91 ee bb 68 b3 e0 35 d1 f0 1e 1f 26 47 ca 96 16 86 e4 80 a0 58 f1 b8 22 20 10 26 9d 38 e9 93 d3 9a e5 0e 43 1f 8f f6 39 c0 f6 f0 c2 7e 4d f0 fc c1 50 9b f9 06 8c 9e a3 c0 6d 36 a9 6a 26 9c 61 04 c0 fe b5 e4 15 9f 14 7d df e8 ab b7 01 03 af 57 73 04 53 14 fb ec 0a 64 04 23 10 98 47 0f 20 f5 08 04 33 cd bb 1e 9d f9 89 10 19 a8 88 1e 81 f9 08 e0 f6 29 ce 7c aa c9 e2 fd 1b 55 09 31 3e 0c c5 cf 5d c4 cb 9d 89 e1 08 00 f0 db 19 71 4d d2 c1 bb 80 77 4d dc 27 3d 6b 02 47 62 5c 19 10 0d 18 13 90 ed 2c d6 0e c5 9a ef b6 72 33 7d cb aa 3f ab 32 3a 31 05 40 60 77 76 2e f6 f0 d5 42 fd fa b9 aa b0 bb 0a 99 0f c5 3f 8a 00 00 09 e2 fa b3 95 46 33 e7 e0 01 51 b1 2f 2d 87 30 4c 18 82 f4 e0 34 e2 be bc 87 87 2f 91 d0 e7 f9 aa c9 6b 7a c4 09 29 80 7b fe 47 6f 6a ae d5 90 04 59 8b 0c 11 df 3 d ae 39 42 cd 88 a9 e3 ca 6d 4a f8 15 3f f6 4b d9 ad f3 f6 38 d0 79 eb e8 7b a7 a4 b1 2a 29 60 f4 eb f3 8f e5 eb 36 8c d6 c0 ac 1d 9e a8 d3 fa a3 af 72 8d 4f ef 7f cd b9 e7 fa c6 74 57 1e 74 2f c4 2a 35 fc 7b 60 31 f8 d6 a9 34 49 71 09 24 18 03 5e 9b e5 3b 69 fd 6a b5 f7 d0 2c 94 77 51 50 ea e0 3d 7c 22 dc 6e 95 99 1e b7 e2 cb 6c 52 e5 ac 42 47 f7 50 e7 90 0c 43 32 ad 0e bc e7 f0 73 a0 e7 c7 79 ac f8 75 6e 46 5d 62 c9 36 92 e4 f7 8e be 41 b3 cf 47 93 1e 7f a1 7d 6d fe 83 61 b2 76 45 e6 3a 85 80 4a d5 22 d7 55 91 02 00 a3 e3 fb ac a1 a6 f3 37 f6 9f 45 9c 7e f4 24 a7 1a bc 67 8e 2f 03 99 af 45 bf 0e 5c 3a 4d 71 cd 2b 43 af 73 ab b8 4f f8 6a 8f 31 50 f0 b8 33 38 7f 3f f4 9f f5 b7 40 9c ad bf f8 70 30 78 90 cc e8 7f f8 e5 8a ee 77 92 8f f3 18 c8 74 e3 Data Ascii: zXT[$1C7C:)HIHK!J---!%H+{}{33k}@+)@ {~^$uQv.(?>^RURAsp<}m\}PR(1^s`AFO@HDH"8A@SRQQ]*m P <(NH} a`l`$gc?A@M].s@D#UP\[Ejlxjrd]66HAF&<#Ca ]u: Uw0Lp2:MPk&\|g\_+6&&k[bbfli}uijQY6=6Q)HD;$@;pb[c_y> e'~9{yE"xh5&GX" &8C9~MPm6j&a}WsSd#G 3)|U1>]qMwM'=kGb\,r3}?2:1@`wv.B?F3Q/-0L4/kz){GojY=9BmJ?K8y{*)`6r OtWt/*5{`14Iq$^;ij,wQP=\|"nlRBGPC2syunF]b6AG}mavE:J"U7E~$g/E\:Mq+CsOj1P38?@p0xwt

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49722	185.104.29.72	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 21:04:55.581090927 CET	66	OUT	GET /tj/Wp-images/cache/styles.css HTTP/1.1 Accept: text/css, */* Referer: http://nellycoacht.nl/tj/Wp-images/wnb5nmuvvnokqnrkcr2amw74zt.php?0=cm9vdEBub3doZXJlLmNvbQ==&.verify??guce_referrer=aHR0cHM6Ly9sb2dpbi55YWhvby5jb20v&guce_referrer_sig=AQAAABA99NmGR9iNQOyU5ml3ASjQfYjcPATD_A8modgjxpNXYNmo8n5zxdi8EZV7GFYPzoSc_RpMz0hYfdCk0OLmxnMB6tpfZnd5ENcxTcI3e56K0Vz3pSL6PoIoDveE6VV6vAiBzqdjcYAbAHdiaf7gx2w9XRGmCh4orbe2VcZO9aN_ 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: nellycoacht.nl Connection: Keep-Alive Cookie: PHPSESSID=53nuvstp9nkf8a2560pn9snkm3
Jan 27, 2021 21:04:55.631972075 CET	67	IN	HTTP/1.1 200 OK date: Wed, 27 Jan 2021 20:04:55 GMT server: Apache/2 upgrade: h2,h2c connection: Upgrade last-modified: Tue, 26 Jan 2021 21:52:26 GMT etag: "1da-5b9d4ab9b13d1-gzip" accept-ranges: bytes vary: Accept-Encoding,User-Agent content-encoding: gzip content-length: 292 content-type: text/css Data Raw: 1f 8b 08 00 00 00 00 00 00 03 6d 51 c9 6e c3 20 10 3d db 5f 81 54 45 4a a2 10 99 56 b9 e0 af 19 cc d8 46 05 c6 02 b2 b5 ca bf 17 90 9b 56 6a 6f b3 bc 65 96 fd 81 ed a5 54 38 52 c0 1a c2 98 30 b0 cf b6 51 74 e3 d1 7c 18 3f 49 a6 28 68 0c 3c 97 fa f6 d1 b6 8a f4 bd 40 16 d0 ba f6 bb be 6d 1c 84 c9 f8 1a 17 cc 71 09 34 05 8c 91 2b a8 7a 0b 45 93 0c 65 44 40 0b c9 5c 30 93 ae 46 a7 59 b2 53 d7 2d 59 ba 99 d1 4c 73 92 ec 0d 5d ce 14 0c ef 53 a0 b3 d7 7c 20 4b 41 b2 17 21 44 6e ac d9 75 36 09 fb 3f 66 df eb 14 d3 81 7c 42 9f 15 21 a5 b0 d5 90 80 5b 50 68 77 59 45 9b b8 58 b8 4b 36 5a 2c e6 60 cd e4 79 96 74 51 b2 21 b3 30 f4 bf c7 06 15 c9 9e 8b 63 63 71 cc 9a c7 53 1d 33 d1 f2 8c 15 a5 44 ee 99 ae eb 0d 60 87 ed 05 c2 96 f3 5a 39 b0 6e c7 f6 4c 6c ca 18 ce 78 be e2 5e 43 65 39 b8 f1 df 4c d1 75 1b c6 99 40 b7 fb ef 2a eb 19 7e be 21 8a ca e3 0b e4 8c 9e e6 da 01 00 00 Data Ascii: mQn =_TEJVFVjoeT8R0Qt|?I(h<@mq4+zEeD@\0FYS-YLs]S| KA!Dnu6?f|B![PhwYEXK6Z,`ytQ!0ccqS3D`Z9 nLlx^Ce9Lu@*~!

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 27, 2021
21:04:55.673053980 CET</td><td>69</td><td>OUT</td><td>GET /tj/Wp-images/cache/bgr.jpg HTTP/1.1
Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5
Referer: http://nellycoacht.nl/tj/Wp-images/wnb5nmuvvnokqnrkcr2amw74zt.php?0=cm9vdEBub3doZXJlLmNvbQ=
=&.verify??guce_referrer=aHR0cHM6Ly9sb2dpbi55YWhvby5jb20v&guce_referrer_sig=AQAAABA99NmGR9iNQOyU5mI3
ASjQfYjcPATD_A8modgjxpNXYNmo8n5zxdi8EZV7GFYPzoSc_RpMz0hYfdCk0OLmxnMB6tpfZnd5ENcxTcI3e56K0V
z3pSL6PoIoDveE6VV6vAiBzqdjcYAbAHdiaf7gx2w9XRGmCh4orbe2VcZO9aN_
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: nellycoacht.nl
Connection: Keep-Alive
Cookie: PHPSESSID=53nuvstp9nkf8a2560pn9snkm3</td></tr>
<tr><td>Jan 27, 2021
21:04:55.734230042 CET</td><td>71</td><td>IN</td><td>HTTP/1.1 200 OK
date: Wed, 27 Jan 2021 20:04:55 GMT
server: Apache/2
upgrade: h2,h2c
connection: Upgrade
last-modified: Tue, 26 Jan 2021 21:52:26 GMT
etag: "3d14f-5b9d4ab9b13d1"
accept-ranges: bytes
content-length: 250191
content-type: image/jpeg
Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 43 00 03 02 02 02 02 02 03 02 02 02 03 03
03 03 04 06 04 04 04 04 04 08 06 06 05 06 09 08 0a 0a 09 08 09 09 0a 0c 0f 0c 0a 0b 0e 0b 09 09 0d 11 0d 0e 0f 10 10
11 10 0a 0c 12 13 12 10 13 0f 10 10 10 ff db 00 43 01 03 03 03 04 03 04 08 04 04 08 10 0b 09 0b 10 10 10 10 10 10 10 10
10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10
10 10 10 ff c0 00 11 08 04 80 07 80 03 01 22 00 02 11 01 03 11 01 ff c4 00 1e 00 00 02 02 03 01 01 01 01 00 00 00 00 00
00 00 00 00 01 02 03 04 05 06 07 08 09 0a ff c4 00 5d 10 00 01 03 02 04 04 03 05 06 03 04 07 04 06 01 15 01 00 02 11
03 21 04 05 31 41 06 12 51 61 22 71 81 07 13 91 a1 b1 08 14 32 c1 d1 f0 23 42 e1 15 52 62 f1 09 24 33 72 82 92 a2 16 43
b2 c2 25 34 53 63 83 a3 17 35 44 54 73 93 b3 c3 26 27 64 74 d2 18 37 45 84 47 a4 57 b4 f2 ff c4 00 1b 01 01 01 01 01 01
01 01 01 00 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 ff c4 00 35 11 01 00 02 01 03 03 01 05 07 04 03 01 00 03 00 0
0 00 01 11 02 03 21 31 04 12 41 05 13 22 51 61 71 06 32 81 91 a1 b1 f0 14 33 c1 d1 23 42 e1 f1 16 24 34 ff da 00 0c 03 0
1 00 02 11 03 11 00 3f 00 fd 3b 24 9b ec 02 83 9d d0 9b 04 12 09 82 60 2a 9e e9 b4 d8 23 60 91 04 de c8 24 ce 84 42 83
9c 26 40 93 d5 29 9d 77 44 ba 48 99 d1 22 e1 a8 51 98 d7 a4 25 cd db 4f a2 16 9f 37 95 d0 5d d0 59 43 9b bc 12 97 30 ea
86 e9 f3 1d 00 4f 98 eb 2a b0 48 fd 51 cd 3b 84 37 59 26 34 40 71 e8 ab 9b 49 40 76 c6 10 dd 67 34 5a c8 2f f2 50 e6 dc 3
8 74 4a 63 42 25 0d d6 73 3b fb a0 a3 9b c9 57 cd ba 7c c6 f2 77 43 74 cb 8a 5c c4 ff 00 2a 81 3d 10 5d fb 28 6e 91 74 ec
12 e7 25 43 98 e9 21 12 66 0d bd 10 dd 32 4f 40 11 cc 76 22 46 aa 13 dc 23 9b bc 21 ba 7c c7 4f c9 1c c6 2e a0 09 88 99
f3 08 9e e8 6e 9f 31 d4 02 8e 63 ac 28 12 7a 89 44 9d 6c 85 ca 64 9d 3a f5 47 31 be 8a 00 db 51 d5 1c c6 62 47 e8 86 e9
f3 19 d0 23 98 95 19 ee 89 ff 00 12 09 73 4e e8 93 d7 e4 ab 2e 1b 14 cb 88 b4 a0 91 33 7d 77 ba 27 65 5f 37 e8 11 cd 1b
14 4b 58 0f 64 4f c1 42 48 b2 39 86 c8 5c a6 0e 88 04 7c 95 61 dd b7 40 75 f5 88 e8 86 eb 24 22 41 3a a8 4c a3 9a da 21
72 9c 8d 01 f4 41 22 62 c5 56 5c 99 74 5c 21 72 9c 82 23 d1 39 07 43 ba af 9c 74 d9 1c d6 98 42 e5 39 1f 05 17 19 b5 a3
55 17 3f f7 2a 25 d7 22 10 b1 20 f4 f4 51 70 fe 64 c9 9d b6 9f e8 a1 cf 36 82 42 17 24 f8 8e 60 74 fa 2a 9d 03 4d 22 ca 64
90 41 02 c7 a9 50 77 40 10 95 47 cb cb ba 85 88 fe aa 6e 9d fa 4d fa 2a 89 e8 85 91 80 54 4d ad bf 4e 89 9d 2c 7e 6a 26
e6 21 10 6a 0d d5 6e 8d b4 3d d4 89 ec a0 e9 37 02 e8 20 eb 1b 5c aa 9f 6d 0a b1 d7 11 01 52 e3 36 9e d0 8b ba 24 ce
91 a2 89 b8 b9 f8 ee 83 f1 1d 52 70 f8 f5 42 51 9d 52 31 02 0e a9 3a 45 8a 8c b8 fe f7 42 8d d1 d7 b0 55 98 1a 91 7d d4
9c 7b aa dd 7e e7 74 44 a4 7a 22 44 1b 95 09 24 4f 2e bd 77 40 26 7e 48 26 39 40 fc d0 0b 4f f5 0a 12 2e 47 aa 39 8f 9c
77 41 3f 84 f7 51 2f 07 7b 44 a8 17 98 8b c9 f9 25 24 c1 84 5a 95 9f bf 34 02 0c c9 f4 55 c9 3a 88 f5 47 31 27 63 3f 24 29
67 30 bc c4 f9 a0 b8 6a 76 55 f3 45 80 04 f9 a3 98 18 82 2f dd 13 85 a0 de d7 44 82 6d be a7 b2 af 9a 75 d3 64 07 4e b1
7d 11 56 f3 03 72 e0 07 c5 00 80 3e aa 1c c6 d6 48 99 b6 9f 54 25 64 8d 09 84 49 90 74 9f 92 ac 3a c4 fe e5 32 f8 be 90
88 b3 99 c1
Data Ascii: JFIFCC"]!1AQa"q2#BRb$3rC%4Sc5DTs&'dt7EGW5!1A"Qaq23#B$4?;$`*#`$B&@)wDH"Q%O7]YC0
O*HQ;7Y&4@qI@vg4Z/P8tJcB%s;W|wCt*=](nt%C!f2O@v"F#!|O.n1c(zDld:G1QbG#sN.3}w'e_7KXdOBH9\|a@u$"A:L!rA"
bV\t\!r#9CtB9U?*%" Qpd6B$`t*M"dAPw@GnM*TMN,~j&!jn=7 \mR6$RpBQR1:EBU}{~tDz"D$O.w@&~H&9@O.G9wA?
Q/{D%$Z4U:G1'c?$)g0jvUE/DmudN}Vr>HT%dIt:2</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49724	185.104.29.72	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 27, 2021
21:05:00.267261028 CET</td><td>558</td><td>OUT</td><td>GET /tj/Wp-images/load.php?0=cm9vdEBub3doZXJlLmNvbQ==&guce_referrer=aHR0cHM6Ly9sb2dpbi55YWhvby5jb20v
&guce_referrer_sig=AQAAABA99NmGR9iNQOyU5mI3ASjQfYjcPATD_A8modgjxpNXYNmo8n5zxdi8EZV7GFYPzoS
c_RpMz0hYfdCk0OLmxnMB6tpfZnd5ENc 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: nellycoacht.nl
Connection: Keep-Alive
Cookie: PHPSESSID=53nuvstp9nkf8a2560pn9snkm3</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 21:05:00.322030067 CET	559	IN	HTTP/1.1 302 Moved Temporarily date: Wed, 27 Jan 2021 20:05:00 GMT server: Apache/2 x-powered-by: PHP/7.0.33 expires: Thu, 19 Nov 1981 08:52:00 GMT cache-control: no-store, no-cache, must-revalidate pragma: no-cache upgrade: h2,h2c connection: Upgrade location: o79foe1v8q20hd8rcawv6gklro.php?0=cm9vdEBub3doZXJlLmNvbQ==&.verify??guce_referrer=aHR0cHM6Ly9sb2dpbi55YWhvby5jb20v&guce_referrer_sig=AQAAABA99NmGR9iNQOyU5mI3ASjQfYjcPATD_A8modgjxpNXYNmo8n5zxdi8EZV7GFYPzoSc_RpMz0hYfdCk0OLmxnMB6tpfZnd5ENcxTcI3e56K0Vz3pSL6PoIoDveE6VV6vAiBzqdjcYAbAHdiaf7gx2w9XRGmCh4orbe2VcZO9aN_ vary: User-Agent content-length: 0 content-type: text/html; charset=UTF-8
Jan 27, 2021 21:05:00.326133013 CET	562	OUT	GET /tj/Wp-images/o79foe1v8q20hd8rcawv6gklro.php?0=cm9vdEBub3doZXJlLmNvbQ==&.verify??guce_referrer=aHR0cHM6Ly9sb2dpbi55YWhvby5jb20v&guce_referrer_sig=AQAAABA99NmGR9iNQOyU5mI3ASjQfYjcPATD_A8modgjxpNXYNmo8n5zxdi8EZV7GFYPzoSc_RpMz0hYfdCk0OLmxnMB6tpfZnd5ENcxTcI3e56K0Vz3pSL6PoIoDveE6VV6vAiBzqdjcYAbAHdiaf7gx2w9XRGmCh4orbe2VcZO9aN_ 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: nellycoacht.nl Connection: Keep-Alive Cookie: PHPSESSID=53nuvstp9nkf8a2560pn9snkm3
Jan 27, 2021 21:05:00.380420923 CET	563	IN	HTTP/1.1 200 OK date: Wed, 27 Jan 2021 20:05:00 GMT server: Apache/2 x-powered-by: PHP/7.0.33 upgrade: h2,h2c connection: Upgrade vary: Accept-Encoding,User-Agent content-encoding: gzip content-length: 348 content-type: text/html; charset=UTF-8 Data Raw: 1f 8b 08 00 00 00 00 00 00 03 5d 51 4d 4b c4 30 10 3d 6f 7f 45 cc 41 f4 d0 cd 82 88 da 6d 56 10 3c 28 22 88 08 e2 2d 4d a6 49 b4 f9 20 99 56 56 f1 bf db 0f 3d e8 25 33 93 37 f3 de 4b a6 a8 0f 54 90 b8 8f 40 0c ba 6e 57 d4 4b 58 d5 06 84 1a e3 aa 76 80 82 48 23 52 06 e4 b4 c7 b6 3c a7 33 80 16 3b d8 3d 5a ed c9 8d 27 18 c8 53 54 02 a1 66 0b 30 b5 74 d6 bf 91 04 1d a7 d9 84 84 b2 47 62 65 f0 94 4c 8a 9c 5a 27 34 b0 e8 35 25 26 41 cb a9 41 8c 15 63 ac 15 c3 d4 b7 1e 0f ca fe 33 e1 be 83 6c 00 f0 77 4a 0a 69 80 cd f7 6b 99 f3 e2 6e 2e a7 ac 09 6a 5f 7c 16 2b 27 92 b6 be 22 9b 6d b1 8a 42 29 eb f5 52 34 42 be e9 14 7a af 2a d2 a7 ee 28 43 1a 98 0b 0a 58 a3 d7 af 51 1f fb 50 26 88 20 f0 4f 73 99 ed 07 54 44 86 01 d2 08 b4 c1 63 d9 0a 67 bb 7d 45 b2 f0 b9 1c 79 6c bb 2d be 26 37 ec d7 4e cd 7e 3e b6 9e 7c cd 4e 6d 9b 84 03 92 93 1c 1f 97 e4 3a 9a 78 b9 e1 d2 5d 0c ea fa aa 6f 4e 54 78 79 be ed ee dc fd d0 3c 70 7e 28 f8 86 92 77 ab d0 70 7a 72 36 e6 06 ac 36 e3 6a 4e 4f 37 74 57 b3 85 6e 96 5a 24 46 c9 79 a7 df 63 7d 1d 7f ec 01 00 00 Data Ascii:]QMK0=oEAmV<("-MI VV=%37KT@nWKXvH#R<3;=Z'STf0tGbeLZ'45%&AAc3lwJikn.j_|+'"mB)R4Bz*(CXQP&OsTDcg}Eyl-&7N~>|Nm:x]oNTxy<p~(wpzr66jNO7tWnZ$Fyc}
Jan 27, 2021 21:05:00.389180899 CET	564	OUT	GET /tj/Wp-images/cache/style.css HTTP/1.1 Accept: text/css, */* Referer: http://nellycoacht.nl/tj/Wp-images/o79foe1v8q20hd8rcawv6gklro.php?0=cm9vdEBub3doZXJlLmNvbQ==&.verify??guce_referrer=aHR0cHM6Ly9sb2dpbi55YWhvby5jb20v&guce_referrer_sig=AQAAABA99NmGR9iNQOyU5mI3ASjQfYjcPATD_A8modgjxpNXYNmo8n5zxdi8EZV7GFYPzoSc_RpMz0hYfdCk0OLmxnMB6tpfZnd5ENcxTcI3e56K0Vz3pSL6PoIoDveE6VV6vAiBzqdjcYAbAHdiaf7gx2w9XRGmCh4orbe2VcZO9aN_ 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: nellycoacht.nl Connection: Keep-Alive Cookie: PHPSESSID=53nuvstp9nkf8a2560pn9snkm3

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 21:05:00.439990997 CET	565	IN	HTTP/1.1 200 OK date: Wed, 27 Jan 2021 20:05:00 GMT server: Apache/2 upgrade: h2,h2c connection: Upgrade last-modified: Tue, 26 Jan 2021 21:52:26 GMT etag: "588-5b9d4ab9b13d1-gzip" accept-ranges: bytes vary: Accept-Encoding,User-Agent content-encoding: gzip content-length: 545 content-type: text/css Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 54 51 6f 9b 30 10 7e 5e 24 fe 83 95 68 52 2a 85 8c a4 50 b5 ae f6 b2 bf 31 f5 c1 60 03 d6 1c 9f 65 cc c8 56 f5 bf cf 36 86 04 4a aa 4a 13 02 e1 b3 ef ee bb ef be 73 b4 da 0b a8 b8 fc 01 e7 68 f5 1a ad be 28 68 b8 e1 20 31 22 79 03 a2 35 ec d9 5a 0d 28 8c b2 e4 ab fb 17 ac 34 e3 c2 68 22 9b 12 f4 09 23 ff 2b 88 61 db d8 6e ee dc e7 ce 1d e9 38 35 35 46 f7 59 a2 ce 6e 5d 33 5e d5 36 42 7a 0c 06 45 28 e5 b2 c2 e8 d1 1a 50 1a ac 39 9c e3 86 ff f5 1b 39 68 ca 74 6c 4d 7e 87 14 bf 2a 0d ad a4 18 e9 2a 27 db 64 e7 9e 7d e6 d2 bd 45 ab 7d db 30 dd 57 13 72 1f 92 59 ee d1 10 22 6b 42 79 db 8c 55 c1 6f a6 4b 01 1d 46 35 a7 94 c9 e7 8f 89 29 88 28 b6 b1 8f f9 ed 78 77 e1 c8 db 6d 48 14 23 57 7c 80 57 1f 7b 6c 27 a2 2d f1 18 25 13 0e 12 fb 0c c4 14 20 40 63 b4 61 25 a3 a9 3f 66 d8 d9 c4 44 f0 ca fa 15 4c 1a a6 43 c9 43 13 91 fa 30 b8 5b 95 20 4d dc 05 22 72 10 f4 3a 55 59 96 f3 88 5c aa d6 cc e9 f4 34 f5 49 6c 5b 8c 01 2b 80 00 fb bd f3 4f f3 47 b1 ef 6b 07 7e fd b2 bb b5 ad 48 d3 74 b6 1d eb 97 3e 59 df 1a 8c 24 48 76 d5 aa 21 db c1 6a c5 f6 81 d3 01 f4 44 17 5e 8c 8a 68 cb 91 6f 68 6b 04 97 ec 12 6c 14 e1 8c ea 10 ca 73 64 d5 67 3d 0e 0f 43 55 18 2b 41 0a 56 5b ca 06 7d 05 37 af c2 63 96 ed 86 f7 a2 c5 c5 52 9b 36 3f 71 73 ab d0 ff 07 3b a1 62 93 24 c5 d3 e1 e0 1d 5b dd 38 4f 05 3c 68 e7 13 20 71 ed c6 21 40 9d c4 4d 1f ee 93 62 06 68 41 40 64 c2 d5 12 ea b4 47 bd a8 4c 2f 79 ca 0a d0 a4 1f bf c0 ca 9b 03 bf e9 34 c8 ea f5 d6 64 8c fd 61 74 9e 32 eb 53 06 09 fb 31 b6 13 3c 31 be d7 75 b4 e2 a5 26 27 b6 d4 b5 e5 fb 61 38 95 8c 97 c5 31 bb ba 45 53 3f 48 36 f2 3f 8b e1 27 a0 88 05 00 00 Data Ascii: TQo0~^$hR*P1`eV6JJsh(h 1"y5Z(4h"#+an855FYn]3^6BzE(P99htlM~**'d}E}0WrY"kByUoKF5)(xwmH#W\|W{l'-%@ca%?fDLCC0[M"r:UY\4Il[+OGk~Ht>Y$Hv!jD^hohklsdg=CU+AV[}7cR6?qs;b$[8O<h q!@MbhA@dGL/y4dat2S1<1 u&'a81ES?H6?'
Jan 27, 2021 21:05:00.447810888 CET	566	OUT	GET /tj/Wp-images/src.php?0=cm9vdEBub3doZXJlLmNvbQ==&a=0 HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: http://nellycoacht.nl/tj/Wp-images/o79foe1v8q20hd8rcawv6gklro.php?0=cm9vdEBub3doZXJlLmNvbQ==&.verify??guce_referrer=aHR0cHM6Ly9sb2dpbi55YWhvby5jb20v&guce_referrer_sig=AQAAABA99NmGR9iNQOyU5mI3ASjQfYjcPATD_A8modgjxpNXYNmo8n5zxdi8EZV7GFYPzoSc_RpMz0hYfdCk0OLmxnMB6tpfZnd5ENcxTcI3e56K0Vz3pSL6PoIoDveE6VV6vAiBzqdjcYAbAHdiaf7gx2w9XRGmCh4orbe2VcZO9aN_ 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: nellycoacht.nl Connection: Keep-Alive Cookie: PHPSESSID=53nuvstp9nkf8a2560pn9snkm3
Jan 27, 2021 21:05:00.502197981 CET	570	IN	HTTP/1.1 200 OK date: Wed, 27 Jan 2021 20:05:00 GMT server: Apache/2 x-powered-by: PHP/7.0.33 upgrade: h2,h2c connection: Upgrade vary: Accept-Encoding,User-Agent content-encoding: gzip content-length: 359 content-type: text/html; charset=UTF-8 Data Raw: 1f 8b 08 00 00 00 00 00 03 75 92 4d 4e c3 30 10 85 d7 a9 d4 3b 18 ef a9 a5 ae 10 72 02 02 b1 47 e2 04 ae 3d ad 2d 6c 8f b1 27 fd d9 71 16 8e c6 49 70 9a a4 02 04 52 94 58 33 9e f7 f9 3d 67 b9 90 57 06 35 9d 12 30 4b c1 77 cb 85 9c be 8d b4 a0 cc b0 68 64 00 52 4c 5b 95 0b 50 cb 7b da 5e df f0 b1 e3 5d 7c 65 19 7c cb 0b 9d 3c 14 0b 40 9c d9 0c db 96 6b a5 2d 88 73 7d bd d2 a5 9c 47 a4 98 65 e5 06 cd 69 54 31 6e cf b4 57 a5 b4 dc e3 ce c5 07 3c 8e fa 8d 74 61 c7 4a d6 2d b7 44 e9 56 08 b1 55 7b a7 31 ae ea 8b cf 43 7d 81 3c 0f d8 75 f7 e2 76 91 b9 c8 08 59 dd 49 2e f6 50 b1 eb 69 c3 16 73 60 4a 93 c3 58 4f 1d cd 2a d9 74 57 01 ac ba b4 68 5a 9e b0 d0 a4 d6 c8 d4 3d 05 e5 bc 14 69 ae b8 98 7a 62 43 64 2d 27 38 56 bb b9 3a c2 e8 4f 2c aa 50 8b c0 59 f2 4a 83 45 6f 20 b7 9c b3 bd f2 7d 6d 64 44 ba 8f 78 b0 90 61 a5 31 7c 83 3c 57 1f 07 cc e6 1f 4e 9a da 7c 42 a4 01 fa d6 bb 0c e6 27 eb f3 fd e3 d7 73 81 0c 21 bb 6a ef 90 31 ee 78 c7 a4 a8 95 bf 60 a5 df 04 47 33 ea 72 fa c7 29 ca 59 70 4c 53 0c 71 8e b7 38 eb 49 31 dd 6c 0d 7d fc 97 be 00 bc 9d 1d f0 67 02 00 00 Data Ascii: uMN0;rG=-l'qIpRX3=gW50KwhdRL[P{^]|e|<@k-s}GeiT1nW<taJ-DVU{1C}<uvYI.Pis`JXO*tWhZ=izbCd-'8 V:O,PYJEo }mdDxa1|<WN|B's!j1x`G3r)YpLSq8I1l}g
Jan 27, 2021 21:05:00.509582996 CET	570	OUT	GET /tj/Wp-images/cache/style2.css HTTP/1.1 Accept: text/css, */* Referer: http://nellycoacht.nl/tj/Wp-images/src.php?0=cm9vdEBub3doZXJlLmNvbQ==&a=0 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: nellycoacht.nl Connection: Keep-Alive Cookie: PHPSESSID=53nuvstp9nkf8a2560pn9snkm3

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 21:05:00.565709114 CET	585	IN	HTTP/1.1 200 OK date: Wed, 27 Jan 2021 20:05:00 GMT server: Apache/2 upgrade: h2,h2c connection: Upgrade last-modified: Tue, 26 Jan 2021 21:52:26 GMT etag: "658-5b9d4ab9b13d1-gzip" accept-ranges: bytes vary: Accept-Encoding,User-Agent content-encoding: gzip content-length: 596 content-type: text/css Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 54 51 6f da 30 10 7e 1e 12 ff c1 02 4d 02 89 74 81 92 6a 4b b5 97 fd 8d a9 0f 4e ec 24 16 c6 67 39 ce 80 56 fc f7 9d 1d 27 40 1a da 49 53 04 8a ef 72 77 df 7d f7 9d 33 60 a7 e9 e4 6d 3a f9 b2 a7 a6 14 2a 25 f1 33 1e 34 65 4c a8 b2 3d e1 b9 00 65 a3 82 ee 85 3c a5 a4 a6 aa 8e 6a 6e 44 81 ce f3 74 f2 20 01 23 7f c1 b1 4d a4 a1 16 56 00 a6 a2 59 0d b2 b1 dc 65 b4 a0 53 92 c4 5f dd bb e4 85 ed 0f d6 60 ba 02 cc 3e 25 fe 55 52 cb 17 11 3a 57 ee 6f e9 3e 39 08 66 ab 94 3c 26 b1 3e ba 73 c5 45 59 61 86 ed 26 18 7a b8 df d1 40 b6 c1 9a c1 31 aa c5 ab 77 64 60 18 37 11 9a bc 87 e6 bb d2 40 a3 58 4a 4c 99 d1 45 bc 72 cf 43 b2 0c 1d 35 d8 5e db 4d a8 bd 8e 07 b5 7b 43 c8 6c 28 13 4d dd 77 05 7f b8 29 24 1c 52 52 09 c6 b8 7a fe 98 98 9c ca 7c 11 f9 9c df 36 cb 0b 47 de 8e 29 49 44 5c f3 01 5e b5 f9 70 64 f8 74 c4 e4 20 c1 a4 64 ce 0b ce b6 fe 33 cb 8f 36 a2 52 94 18 97 73 65 b9 19 0c 91 e8 cf f4 d0 aa e1 10 88 c8 40 b2 eb 52 45 31 94 05 11 4a 37 76 48 a7 a7 a9 2d 82 63 b1 16 50 00 01 f6 fb e0 df f6 a4 f9 cf 99 03 3f 7b 59 dd 73 6b 5a d7 07 1c c7 ec a5 2d d6 8e 26 25 0a 14 bf 1a 55 57 6d 8d 5a c1 39 08 d6 81 be d1 85 17 a3 a6 06 39 f2 03 6d ac 14 8a 5f 92 f5 22 1c 50 1d 52 79 8e 50 7d 18 b1 7e ea ba 4a 53 2d 69 ce 2b a4 ac d3 57 08 f3 2a dc 24 c9 aa fb 5d b4 38 da 6a dd 64 7b 61 ef 35 fa ff 60 6f a8 98 c7 71 fe 63 bd f6 81 8d a9 5d a4 06 11 b4 f3 0f 20 d3 ca ad 43 80 7a 93 77 fb f4 18 e7 03 40 23 02 a2 37 5c 8d a1 de b6 a8 47 95 e9 25 cf 78 0e 86 b6 eb 17 58 39 3b f0 f3 83 01 55 be dd db 8c 7e 3e 9c 0d 4b 26 6d c9 20 61 bf c6 b8 c1 37 c6 f7 ba fe 58 d9 0e c6 85 64 05 11 33 a0 31 10 5b ca 76 c2 62 91 26 af 22 bc 14 24 4e b8 ef a3 f3 ba 4b 0b ef 65 c9 f3 2b df ae b2 7b 39 ee da c3 eb 1d 47 3d 6e 87 51 f3 98 ed fc 17 4b 11 8e e8 58 06 00 00 Data Ascii: TQo0~MtjKN$g9V'@ISrw}3`m:*%34eL=e<jnDt #MVYeS_`>%UR:Wo>9f<&>sEYa&z@1wd`7@XJLEr C5^M{Cl(Mw)$RRz|6G)ID\^pdt d36Rse@RE1J7vH-cP?{YskZ-&%UWmZ99m_"PRyP}~JS-i+W*$]8jd{a5`oqc] C zw@#7\G%xX9;U~>K&m a7Xd31[vb&"$NKe+{9G=nQKX

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49733	185.104.29.72	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 21:05:00.498182058 CET	569	OUT	GET /tj/Wp-images/serv/mode/bg.jpg HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: http://nellycoacht.nl/tj/Wp-images/o79foe1v8q20hd8rcawv6gklro.php?0=cm9vdEBub3doZXJlLmNvbQ==&.verify??guce_referrer=aHR0cHM6Ly9sb2dpbi55YWhvby5jb20v&guce_referrer_sig=AQAAABA99NmGR9iNQOyU5mI3ASjQfYjcPATD_A8modgjxpNXYNmo8n5zxdi8EZV7GFYPzoSc_RpMz0hYfdCk0OLmxnMB6tpfZnd5ENcxTcI3e56K0Vz3pSL6PoIoDveE6VV6vAiBzqdjcYAbAHdiaf7gx2w9XRGmCh4orbe2VcZO9aN_ 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: nellycoacht.nl Connection: Keep-Alive Cookie: PHPSESSID=53nuvstp9nkf8a2560pn9snkm3

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 27, 2021
21:05:00.548207045 CET</td><td>572</td><td>IN</td><td>HTTP/1.1 200 OK
date: Wed, 27 Jan 2021 20:05:00 GMT
server: Apache/2
upgrade: h2,h2c
connection: Upgrade
last-modified: Tue, 26 Jan 2021 21:52:26 GMT
etag: "2e5c9-5b9d4ab9b1f89"
accept-ranges: bytes
content-length: 189897
content-type: image/jpeg
Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 60 00 60 00 00 ff db 00 43 00 04 02 03 03 03 02 04 03 03 03 04 04 04 04 05 09 06 05 05 05 05 0b 08 08 06 09 0d 0b 0d 0d 0d 0b 0c 0c 0e 10 14 11 0e 0f 13 0f 0c 0c 12 18 12 13 15 16 17 17 17 0e 11 19 1b 19 16 1a 14 16 17 16 ff db 00 43 01 04 04 04 05 05 05 0a 06 06 0a 16 0f 0c 0f 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 ff c0 00 11 08 04 b0 07 80 03 01 22 00 02 11 01 03 11 01 ff c4 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b ff c4 00 b5 10 00 02 01 03 03 02 04 03 05 05 04 04 00 00 01 7d 01 02 03 00 04 11 05 12 21 31 41 06 13 51 61 07 22 71 14 32 81 91 a1 08 23 42 b1 c1 15 52 d1 f0 24 33 62 72 82 09 0a 16 17 18 19 1a 25 26 27 28 29 2a 34 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e1 e2 e3 e4 e5 e6 e7 e8 e9 ea f1 f2 f3 f4 f5 f6 f7 f8 f9 fa ff c4 00 1f 01 00 03 01 01 01 01 01 01 01 01 01 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b ff c4 00 b5 11 00 02 01 02 04 04 03 04 07 05 04 04 00 01 02 77 00 01 02 03 11 04 05 21 31 06 12 41 51 07 61 71 13 22 32 81 08 14 42 91 a1 b1 c1 09 23 33 52 f0 15 62 72 d1 0a 16 24 34 e1 25 f1 17 18 19 1a 26 27 28 29 2a 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 82 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e2 e3 e4 e5 e6 e7 e8 e9 ea f2 f3 f4 f5 f6 f7 f8 f9 fa ff da 00 0c 03 01 00 02 11 03 11 00 3f 00 fa 29 d2 a9 dc a5 5e 6f b9 55 6e 12 bc b3 d6 31 75 5b 74 92 36 4a f2 5f 89 7a 1f d9 e4 6b 98 93 e5 7f bf fe fd 7b 25 e2 57 27 e2 db 48 ae ec e4 8a 54 fb f4 12 7c d3 e3 0b 4f dd c8 95 e4 be 2a b7 d8 f2 25 7b d7 8e 6c bc a9 24 89 ff 00 82 bc 6f c6 76 fb 24 6a ee c3 c8 e1 c4 c4 f3 39 93 64 8c 94 da b5 aa c7 e5 de 35 55 af 46 27 96 14 25 14 e4 a6 03 92 ac 43 25 55 a7 25 00 69 43 2d 4c 97 15 96 8f 4e 49 2a 39 4b e6 35 92 e2 9d f6 8a c9 f3 29 c9 2b ff 00 7e a7 94 bf 6a 6b 7d a2 a4 f3 7f db ac 74 9e 9d e7 3d 1c a1 ed 4d 8f 37 fd ba 91 2e 2b 17 ed 0f 4e 4b 87 a3 94 af 68 6d 25 c5 48 97 15 86 97 0f 4e 4b b7 a3 94 39 cd c4 b8 a7 7d a2 b0 fe d2 f5 22 5d d1 ca 1c e6 e2 5c 53 92 e3 fd ba c3 fb 65 3b ed 95 3c a3 e6 37 92 ee 9c 97 75 85 f6 ca 54 bc a6 1c c7 40 97 7f ed d3 92 ef fd ba c1 4b cd 94 ef b6 50 1c c7 40 97 75 22 5d ed ae 77 ed d5 2f db 7f db a0 39 8e 87 ed 7f ed d4 89 79 5c da 5e 7f b7 52 fd b7 fd ba 39 86 74 69 79 52 fd b2 b9 af b6 d2 fd b7 fd ba be 60 3a 54 bc a7 7d b2 b9 b4 bd a7 7d ba 8e 60 3a 64 bc a7 25 e5 73 3f 6e a9 12 f7 fd ba 39 8a 3a 64 bc a9 3e d9 5c ba de ff 00 b7 4f fb 6f fb 74 73 01 d2 fd b2 9d f6 cf f6 eb 99 fe d0 f6 a7 25 ef fb 74 73 01 d3 7d b2 8f b6 7f b7 5c d7 db 7f db a4 fe d0 ff 00 6e ab 98 0e a1 2f 69 c9 78 95 cc 7f 68 7f b5 4a b7 bf ed d1 cc 47 29 d4 25 ea 7f 7e 9c 97 a8 f5 ca ff 00 68 7b 54 89 a9 d1 ed 06 75 09 78 9f df a9 7e
Data Ascii: JFIF``CC"}!1AQa"q2#BR$3br%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyzw!1AQaq"2B#3Rbr$4%&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz?)^oUn1u[t6J_zk{%W'HT|O*%{lovj9d5UF'%C%U%iC-LNI*9K5)+~jk}t=M7.+NKhm%HNK9}"]\Se;<7uT@KP@u"]w/9y\^R9tiyR`:T}}`:d%s?n9:d>\Oots%ts}\n/ixhJG)%~h{Tux~</td></tr>
<tr><td>Jan 27, 2021
21:05:00.768552065 CET</td><td>773</td><td>OUT</td><td>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: nellycoacht.nl
Connection: Keep-Alive
Cookie: PHPSESSID=53nuvstp9nkf8a2560pn9snkm3</td></tr>
<tr><td>Jan 27, 2021
21:05:01.121622086 CET</td><td>779</td><td>IN</td><td>HTTP/1.1 302 Found
date: Wed, 27 Jan 2021 20:05:00 GMT
server: Apache/2
x-powered-by: PHP/7.0.33
link: <https://www.nellycoacht.nl/wp-json/>; rel="https://api.w.org/"
x-redirect-by: WordPress
upgrade: h2,h2c
connection: Upgrade
location: http://www.nellycoacht.nl/wp-includes/images/w-logo-blue-white-bg.png
vary: User-Agent
content-length: 0
content-type: text/html; charset=UTF-8</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49735	185.104.29.72	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 21:05:01.255414009 CET	783	OUT	GET /wp-includes/images/w-logo-blue-white-bg.png 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 Connection: Keep-Alive Host: www.nellycoacht.nl

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 21:05:01.311335087 CET	784	IN	HTTP/1.1 200 OK date: Wed, 27 Jan 2021 20:05:01 GMT server: Apache/2 upgrade: h2,h2c connection: Upgrade last-modified: Thu, 21 May 2020 09:10:12 GMT etag: "1017-5a624e1454500" accept-ranges: bytes content-length: 4119 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 50 00 00 00 50 08 06 00 00 00 8e 11 f2 ad 00 00 0f de 49 44 41 54 78 da e5 5d 09 78 55 c5 15 0e 5b c1 c8 56 10 d1 2a 29 9b 4b 6b ad c5 da 56 ad 6b b5 1b 4a 5d 6a 4b 45 6c 3f f5 ab b5 74 b7 04 12 21 09 7b 14 2c a0 a2 11 45 83 d9 13 b2 90 90 1d 92 40 c0 b0 84 b0 46 90 25 04 08 81 10 12 42 16 12 b2 4e e7 bf 79 93 cc 9d 77 97 b9 f7 bd 87 49 7b be 6f be f0 de 9b 3b cb b9 73 e6 9c f3 9f 33 83 97 d7 57 48 d7 cf 8b 1b ff ad a5 c9 2f d3 b2 7a 42 70 d2 96 6f 2c 58 57 f2 f5 80 98 9a 81 b3 23 5a bd 66 86 11 be 7c 6d 76 44 f3 d0 39 d1 17 46 06 c6 1c a2 cf a5 8d 08 8c 79 ab 9f 6f f8 b3 f4 b7 31 5e ff 37 34 33 6c d8 d8 c5 09 af de f9 76 ca e7 23 03 63 1b 45 26 f1 65 d8 dc 68 55 31 aa 7b 8d 7f e4 05 ca e0 08 fa ef a9 b4 0c f9 5f 63 5a ff fb 57 65 bc 76 fb d2 f5 c5 03 66 85 77 f0 13 1f b3 28 81 fc 36 7c 0b 59 bc e9 20 49 3a 78 9a ec 2d af 26 17 1a ae 90 8e 0e e2 44 f8 0e bf a1 0e ea e2 19 3c 8b 36 f8 36 e9 aa 6c b9 f6 8d a8 54 fa ef 29 b4 f4 eb b5 7c bb fd ad f5 23 9f fc 24 67 1d 15 b7 56 4e 0c c9 93 9f e4 92 0f b7 1f 21 27 2f 36 10 77 11 da 42 9b 68 1b 7d b0 fe 06 f9 45 56 f6 f5 0d f3 a5 ff 1e da 6b 18 37 22 20 66 e8 7d ef a5 47 0e 7e 23 aa 8d 4d e4 fb 2b d3 c8 ea ed 47 c9 a5 a6 16 e2 69 42 1f e8 eb ee 15 a9 5d 8c ec 3f 2b bc 96 fe f5 a3 c5 bb 27 8b 6a 9f 47 42 b2 16 50 25 d0 cc 06 fe ab d0 5c b2 ad f4 bc f4 e4 eb af b4 92 c3 e7 2f 91 cd 25 15 8a 98 26 1c 38 45 12 0f 9e 22 e9 87 cf 90 bc e3 15 a4 b8 a2 86 34 34 b7 4a b7 87 be 31 06 8e 91 15 f4 ef b4 1e c7 bb d7 53 0a 1f a3 8a a1 92 0d f4 b1 d5 d9 64 cf 99 6a c3 c9 5d 6e 69 25 19 5f 96 93 39 19 7b c9 4f 3f da 48 a8 06 36 54 14 7c 41 dd 47 43 b2 95 67 b3 8f 9c 55 18 6f 44 45 74 2c 3f f9 30 bb eb f9 81 7e 11 9b e9 df 71 3d 82 79 cf 7e b6 39 e4 5a ff a8 2e a5 80 15 63 b4 c2 c2 76 97 90 5f ae c9 c1 fe 24 cd 30 b3 32 c0 b1 b7 46 ee 39 61 c8 4c 8c 8d 29 1d aa 6c 2e d3 bf d3 bf 32 c6 8d 9e 17 77 ed 0f df 49 df cf 26 f1 a7 f8 1d a4 56 67 8f fb b2 b2 96 cc 48 dc 49 06 cf 89 72 1b d3 f4 0a d5 c0 e4 2f b4 af 92 aa 7a cd b1 60 8c 18 2b f7 cc 1a 5a 06 5e 55 e6 3d 1a 92 35 61 42 70 62 0d 06 30 3c 20 86 ac 2f 3e ad 39 d8 63 17 ea c8 ef 22 f2 49 1f df 30 8f 33 4e 2c 7d 7d c3 c9 d4 f0 7c 5d 46 62 8f c5 d8 51 b7 cf cc b0 1d f4 ef a8 ab c2 bc 57 e2 0a 1e a1 ab 4f 51 14 df 79 3b 85 1c af aa d3 7c cb 33 37 ec c6 a6 7d d5 19 a7 e1 c1 28 63 d1 b2 00 f0 82 ef 58 96 e2 60 78 58 29 fd 3b d1 a3 cc 0b cc dc fb 3c 35 53 da d1 e1 cf 3e da a4 39 a8 8d 47 cf 3a 19 b7 3d a1 dc bc 30 5e 19 9b 96 d9 f3 f8 ea 8d 6c 5f 3c 47 ff de e2 11 e6 cd 48 dc f1 18 f5 43 15 4f 82 2a 0e d2 dc d6 ae 1a 48 6b 7b 87 f2 a6 7b 1a e3 c4 f2 b7 a4 5d 4e 63 c7 e7 a7 42 f3 98 38 97 bb 7d 25 3e 1d 9a 77 eb 0d f3 e3 5a d0 c1 af 29 f3 da da d5 be 16 5c ac 87 3e c8 ea f1 cc 63 e5 c7 ab 32 c9 f9 fa 26 d5 1c 30 27 c6 44 5a 4a dc b6 27 7e 7b 59 f2 e0 89 c1 49 97 d0 f0 cf 3f de e4 f4 f6 b0 07 de f2 66 52 af 61 1e ca d8 c5 89 e4 8f eb b6 3b 99 3c 98 1b 6c 52 47 bd ed 6e d1 ce f7 bd 97 51 8c 06 bf fb 9f 0d 4e 66 0a 36 e1 9b e8 de d2 5b 18 47 e7 42 76 9d ae 32 75 05 99 62 51 4c 1c 57 88 9a 20 b0 91 08 75 cf c8 89 6a b5 39 50 7a b1 be 57 31 0f e2 29 4a 8f 1e 41 aa 86 77 43 68 f6 8c ed 45 9b 0e 4c 61 1e 46 ea a1 33 aa 0e aa 2e 5f 21 b7 be b5 be d7 30 0f 1a b8 ee 8a 35 20 Data Ascii: PNGIHDRPPIDATx]xU[V*)KkVkJ]jKEl?t!{,E@F%BNywl{o;s3WH/zBpo,XW#Zf|mvD9Fyo1^743lv#cE&ehU1{_ cZWevfw(6|Y I:x-&D<66lT)|#$gVN!'/6wBh}EVk7" f}G~#M+GiB]?+'jGBP%\/%&8E"44J1Sdj]ni%_9{O?H6T|AGCgUoDEt,? 0~q=y~9Z.cv_$02F9aL)|.2wl&VgHIr/z`+Z^U=5aBpb0< />9c"|03N,}}|]FbQWOQy;|37}(cX`xX);<5S>9G:=0^|_<GHCO* Hk{{]NcB8}%>wZ)\>c2&0'DZJ'~{YI?fRa;<lRGnQNf6[GBv2ubQLW uj9PzW1)JAwChELaF3._!05

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 4804 Parent PID: 800

General

Start time:	21:04:52
Start date:	27/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7d4190000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 1852 Parent PID: 4804

General

Start time:	21:04:53
Start date:	27/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4804 CREDAT:17410 /prefetch:2
Imagebase:	0x1330000
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