ID: 383899
Cookbook: browseurl.jbs
Time: 12:03:19
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

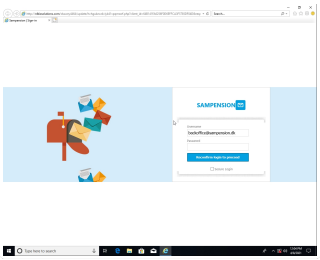
Analysis Report http://nlbizsolutions.com/dsswey4464/u…

Overview

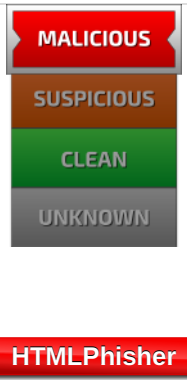
General Information

Sample URL:	http://nlbizsolutions.com/dsswey4464/update?email=backoffice@sampension.dk
Analysis ID:	383899
Infos:	

Most interesting Screenshot:



Detection



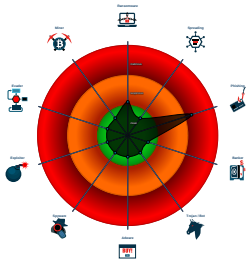
HTMLPhisher

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Yara detected HtmlPhish10
- 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: 6616 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6716 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6616 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

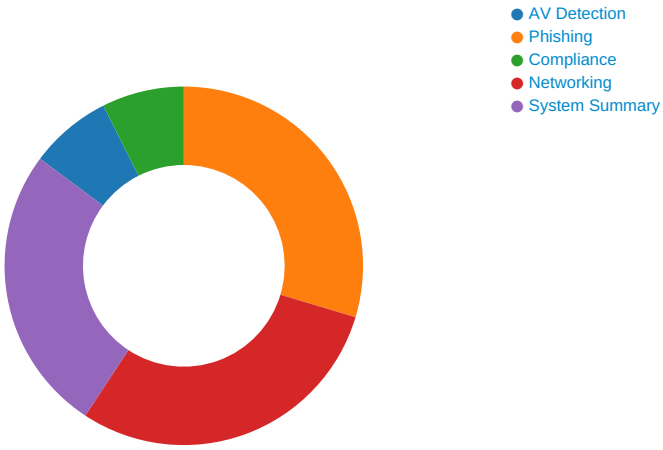
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\hchgukzwr4viyk41vpqmzxrf[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

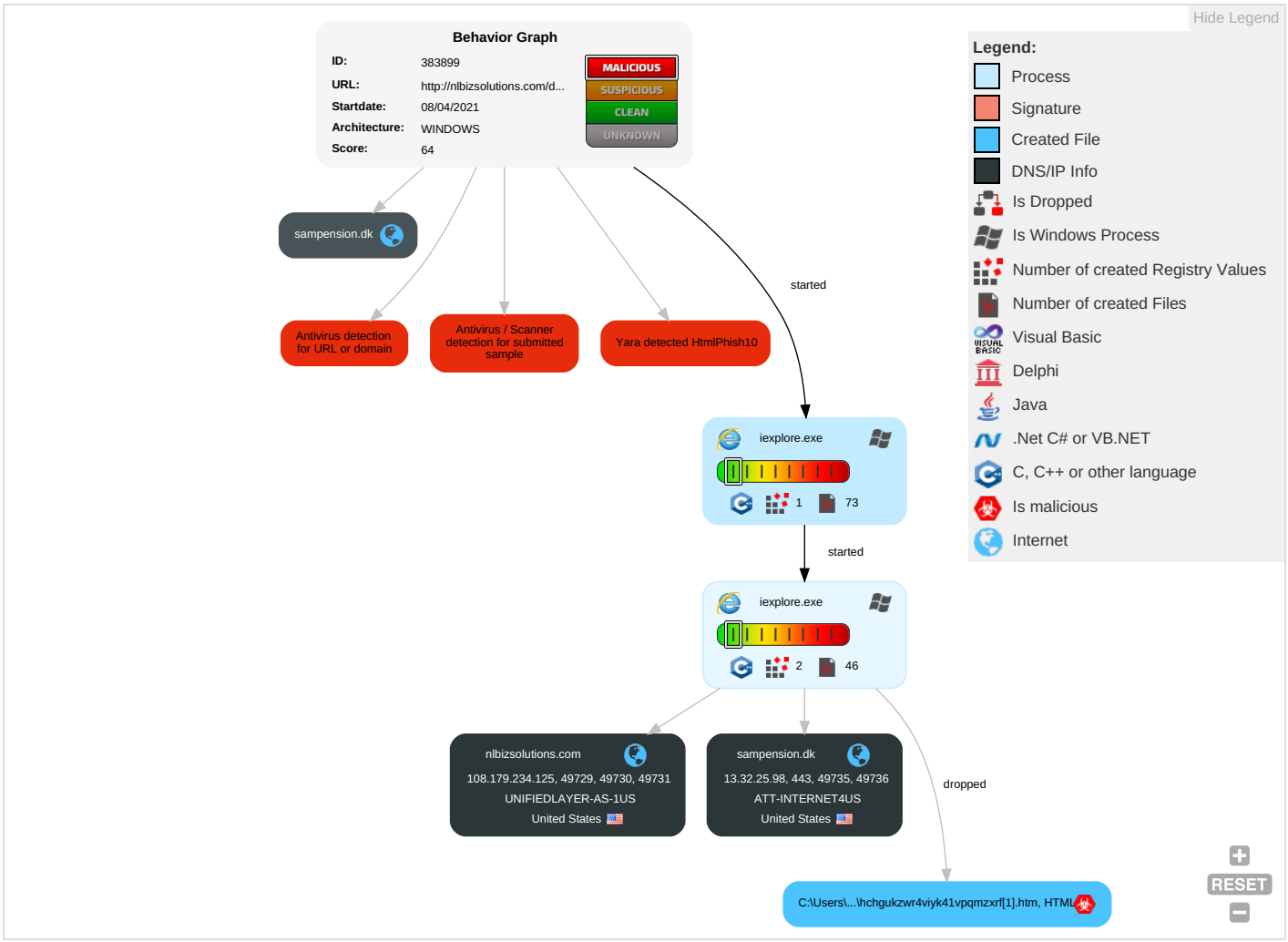
Phishing:

Yara detected HtmlPhish10

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 4	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 5	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 4	SIM Card Swap		Carri Billin Fraud

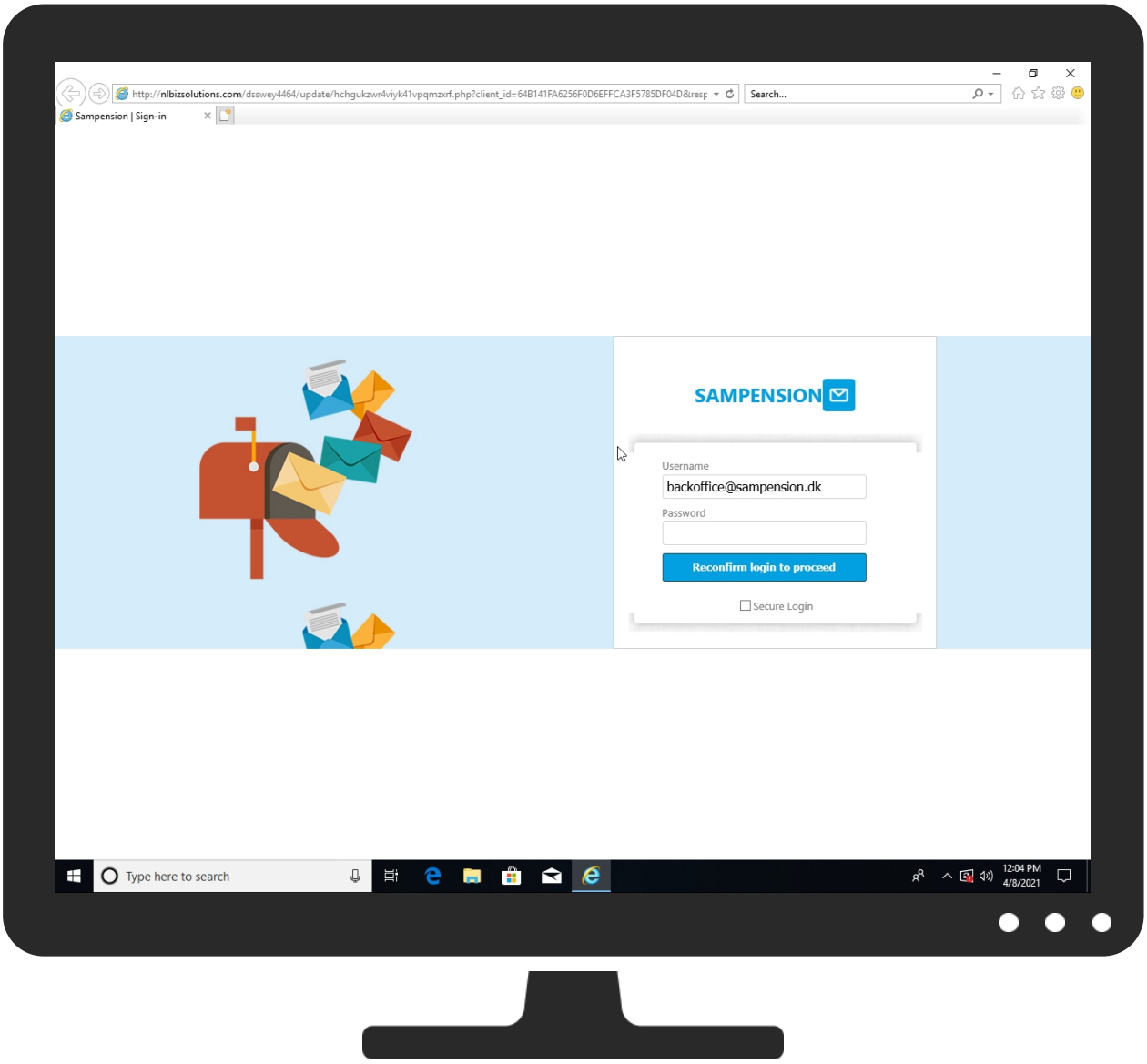
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://nlbizsolutions.com/dsswey4464/update?email=backoffice@sampension.dk	100%	Avira URL Cloud	phishing	
http://nlbizsolutions.com/dsswey4464/update?email=backoffice@sampension.dk	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://nlbizsolutions.com/dsswey4464/update?email=backoffice@sampension.dk	100%	UrlScan	phishing brand: generic generic email	Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
nlbizsolutions.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://nlbizsolutions.com/dsswey4464/update/hchgukzwr4viyk41vpqmzxrf.php?client_id=64B141FA6256F0D6EFFCA3F5785DF04D&response_mode=form_post&response_type=code+id_token&scope=openid+profile&email=backoffice@sampension.dk&Connect_Authentication_Properties&&nonce=50086702864b141fa6256f0d6effca3f5785df04d&redirect_uri=&ui_locales=en-US&mkt=en-US	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://nlbizsolutions.com/dsswey4464/update/login_files/img/middle.png	100%	Avira URL Cloud	phishing	
http://nlbizsolutions.com/dsswey4464/update/?email=backoffice	100%	Avira URL Cloud	phishing	
http://nlbizsolutions.com/favicon.ico	0%	Avira URL Cloud	safe	
http://nlbizsolutions.com/dsswey4464/update/login_files/logo.png	100%	Avira URL Cloud	phishing	
http://nlbizsolutions.com/dsswey4464/update/login_files/loginDialog.js	100%	Avira URL Cloud	phishing	
http://nlbizsolutions.com/dsswey4464/update/login_files/generatedDefaults.js	100%	Avira URL Cloud	phishing	
http://nlbizsolutions.com/dsswey4464/update/login_files/is	100%	Avira URL Cloud	phishing	
http://nlbizsolutions.com/dsswey4464/update/login_files/loginBasic.css	100%	Avira URL Cloud	phishing	
http://nlbizsolutions.com/dsswey4464/update/login_files/bottom.png	100%	Avira URL Cloud	phishing	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://nlbizsolutions.com/dsswey4464/update/hchgukzwr4viyk41vpqmzxrf.php?client_id=64B141FA6256F0D6E	100%	Avira URL Cloud	phishing	
http://nlbizsolutions.com/dsswey4464/update/?email=backoffice@sampension.dk	100%	Avira URL Cloud	phishing	
http://nlbizsolutions.com/dsswey4464/update/login_files/top.png	100%	Avira URL Cloud	phishing	
http://nlbizsolutions.com/dsswey4464/update/login_files/img/background.png	100%	Avira URL Cloud	phishing	
http://nlbizsolutions.com/dsswey4464/update/login_files/loginAdvanced.css	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sampension.dk	13.32.25.98	true	false		high
nlbizsolutions.com	108.179.234.125	true	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

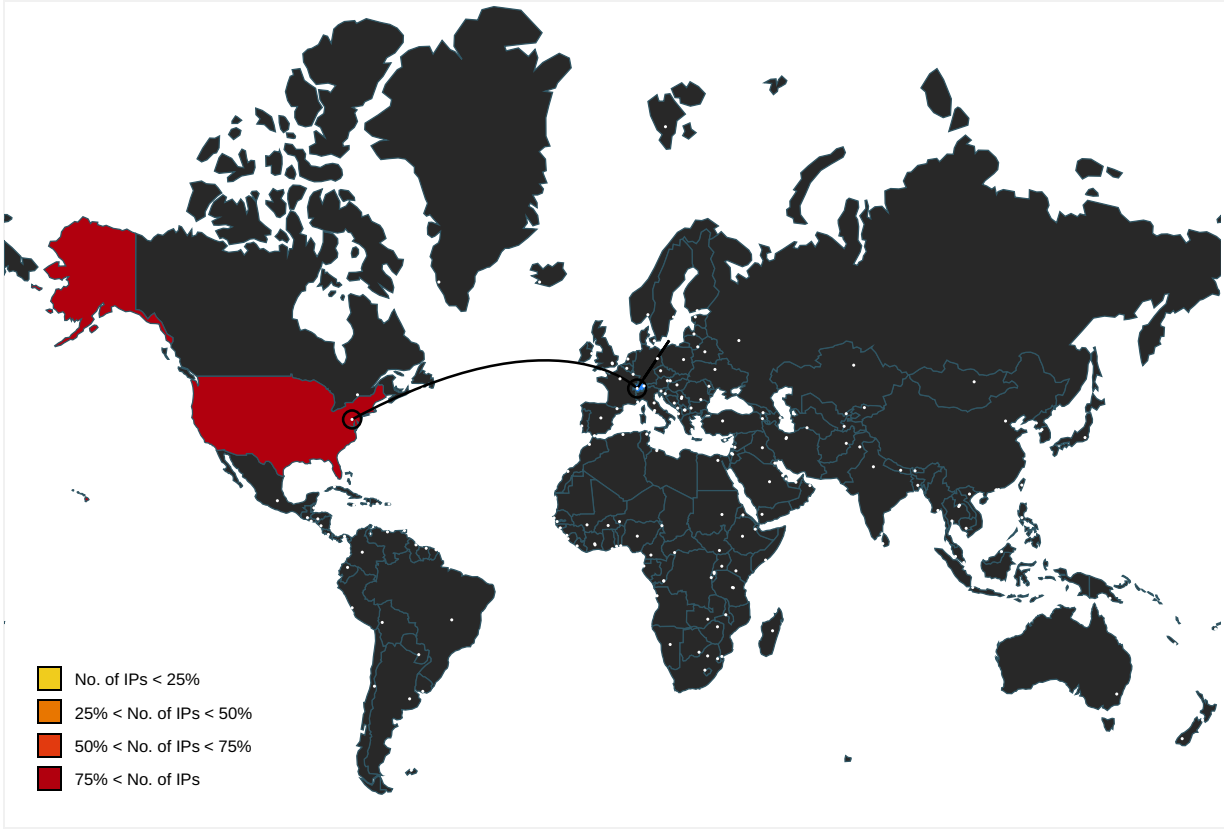
Name	Malicious	Antivirus Detection	Reputation
http://nlbizsolutions.com/dsswey4464/update?email=backoffice@sampension.dk	true		unknown
http://nlbizsolutions.com/dsswey4464/update/login_files/img/middle.png	false	• Avira URL Cloud: phishing	unknown
http://nlbizsolutions.com/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://nlbizsolutions.com/dsswey4464/update/login_files/logo.png	false	• Avira URL Cloud: phishing	unknown
http://sampension.dk/favicon.ico	false		high
http://nlbizsolutions.com/dsswey4464/update/login_files/loginDialog.js	false	• Avira URL Cloud: phishing	unknown
http://nlbizsolutions.com/dsswey4464/update/login_files/generatedDefaults.js	false	• Avira URL Cloud: phishing	unknown
http://nlbizsolutions.com/dsswey4464/update/login_files/is	false	• Avira URL Cloud: phishing	unknown
http://nlbizsolutions.com/dsswey4464/update/login_files/loginBasic.css	false	• Avira URL Cloud: phishing	unknown
http://nlbizsolutions.com/dsswey4464/update/login_files/bottom.png	false	• Avira URL Cloud: phishing	unknown
http://nlbizsolutions.com/dsswey4464/update/?email=backoffice@sampension.dk	false	• Avira URL Cloud: phishing	unknown
http://nlbizsolutions.com/dsswey4464/update/login_files/top.png	false	• Avira URL Cloud: phishing	unknown
http://nlbizsolutions.com/dsswey4464/update/login_files/img/background.png	false	• Avira URL Cloud: phishing	unknown
http://nlbizsolutions.com/dsswey4464/update/login_files/loginAdvanced.css	false	• Avira URL Cloud: phishing	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://nlbizsolutions.com/dsswey4464/update/?email=backoffice	update[1].htm.3.dr	false	• Avira URL Cloud: phishing	unknown
http://www.youtube.com/	msapplication.xml7.1.dr	false		high
http://www.wikipedia.com/	msapplication.xml6.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://nlbizsolutions.com/dsswey4464/update/hchgukzwr4viyk41vpqmzxrf.php?client_id=64B141FA6256F0D6E	~DF0A4DF2C8364664C9.TMP.1.dr, {C2FDE60B-9851-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: phishing	unknown
http://www.amazon.com/	msapplication.xml.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.live.com/	msapplication.xml2.1.dr	false		high
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://www.twitter.com/	msapplication.xml5.1.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.179.234.125	nlbizsolutions.com	United States		46606	UNIFIEDLAYER-AS-1US	false
13.32.25.98	sampension.dk	United States		7018	ATT-INTERNET4US	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383899
Start date:	08.04.2021
Start time:	12:03:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://nlbizsolutions.com/dsswey4464/update?email=backoffice@sampension.dk
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:	11
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.phis.win@3/27@3/2
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.88.21.125, 23.54.113.53, 104.83.120.32, 20.82.210.154, 104.43.193.48, 23.10.249.26, 23.10.249.43, 152.199.19.161, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, go.microsoft.com, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, ie9comview.vo.msecnd.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus15.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, cs9.wpc.v0cdn.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{C2FDE609-9851-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.856537850445688
Encrypted:	false
SSDEEP:	192:r8ZZDZ22iWftfrifUuczMdUBA6DwmNsfLKuhjX:r8FNBFkhWFQ7
MD5:	BCE1D50E35A1483C6362F316BD7CCB11
SHA1:	6E04FCAB7D8BE439C8DC5618FA5171F5501CEEDD
SHA-256:	F7ABEBBBB1EE548D662A540A7A89EB1D165AFDF540D507829334FBDD0C843A1E
SHA-512:	BB3E97619C4B613892BCD54F6346A25ADC793A913B20EE570570E739923BB28C9B97D7F5D7D43C466AA75F22F325B9F97ABC6BC18941D81AB13488AA57D10A2
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\{C2FDE60B-9851-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30770
Entropy (8bit):	2.229883560604403
Encrypted:	false
SSDEEP:	96:rKZZBQHV6jBS4jh2WWfMT9M60vCzq60vCGQ60vCM60vC660vCZ60vClr+b8yWr:rKZZBQHV6jk4jh2WWfMT9x3XKtNLAW2r
MD5:	3A0ED58E4559E30C6E40525341CEF1C2
SHA1:	5EB3FFDF7CF4BD7AA6A9C6B6629C50D6B03A8361
SHA-256:	582F1A67650C6B51CCAAA3A26783F4273702963C33645570A0A4D25B8A46F4F8
SHA-512:	46A50086F3125581AFA4437E1D639D1757FA9D1CA3A0698170F3392C5F989CA7022CD3B62C1EDB0ADF1D56B51B0E25C2D32BA8D9F5ED0773C4B828A65F6BF05
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\{C2FDE60C-9851-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5665551314069739
Encrypted:	false
SSDEEP:	48:IwkjGcprJGwpalmjG4pQ3AGrapbSuGQpKwG7HpRwTGIpG:rkZZjQlmV63eBSmALTkA
MD5:	290F6D4EACA8EBD521381A63A21A14A5
SHA1:	6949846C2EE9AB628F7295A5BA58504D06B6B28D
SHA-256:	3B5711AB09BCFF1DF2DA83A8899EDBB71C334526E99FDCE7DF8295A54C6D470B
SHA-512:	6662B1AFED3EAFCED848410454C70BAC3126D2A6C5C19674C09E9E3E9CB2BCD7432524F73646448BAD70530A7F3D44F6CE98D8D702D0DAE4406CAE1AF81FFA 09
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{C2FDE60C-9851-11EB-90EB-ECF4BBEA1588}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.068995106337389
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEhPnWimI002EtM3MHdNMNxOEhPnWimI00OYGVbkEtMb:2d6NxO0PSZHKd6NxO0PSZ7YLb
MD5:	4084F3386F5E9E9019EFFF5FB2C7A681
SHA1:	12D2B3AF41FE302FABC218D2FB1AD955C4621F4D
SHA-256:	078BEB467ECA6CC055A2A1B4AF5B7B55B68A848A7FA92B505C6BE2B3029E8B8A
SHA-512:	0EF7899450EAC1D91A33CDED4B2F5E8CBD967504C3F7AA97FF6341EA8E16758AC42BAC67061E73212277E61B4E4FC41CAA0C0039DFC473C5FC441D35D2628A 9
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x9a114cf1,0x01d72c5e</date>< accdate>0x9a114cf1,0x01d72c5e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x9a114cf1,0x01d72c5e</date><accdate>0 x9a114cf1,0x01d72c5e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile ></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.086156400864746
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kwUHrnWimI002EtM3MHdNMNxe2kwUHrnWimI00OYGkak6EtMb:2d6Nxr4LSZHKd6Nxr4LSZ7Yza7b
MD5:	B3B0844F97D2AECDBD294C2329CCF587
SHA1:	074457F8A98E86961FB9628F6BAC40CE462DBD6D
SHA-256:	8793E3374161CA9E0B42009C294A05EB1CC9F5BA44E454EB05F32364CA8A2A1B
SHA-512:	08B5A5E4AC49CD15AAE4461DFBCA0F3C8F7D1D1255E811664F50F94E31D5FC2394EE4CDF9DBB34620AC4E7ACD8CDC241C72FC4F810DB57289973A1080141 3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x9a0a25e3,0x01d72c5e</date><a ccdate>0x9a0a25e3,0x01d72c5e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x9a0a25e3,0x01d72c5e</date><a ccdate>0x9a0a25e3,0x01d72c5e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Am azon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.080968773593659
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLawFJwEnWimI002EtM3MHdNMNxvLawFJwEnWimI00OYGmZEtMb:2d6Nxv1fSZHKd6Nxv1fSZ7Yjb
MD5:	87F73422ABAAE4ECB27F8F502C621486
SHA1:	65F9C0A9EFBD26A5C184311F0A52CB90EEBC580E
SHA-256:	E97ADCBA20AB8AAC81C692ECCD86C3ECD9B7C6AA5517966177BFB27F12DEA049
SHA-512:	7F232EF9E7DA0BAE974E7544E373489B979BF7A9E6886A5BE5646C5DF82C4612143BFC06FAD883E9698AA69962E665EEB4444A1B2EDC106F7201F787C87B3212
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x9a13af3f,0x01d72c5e</date> <accdate>0x9a13af3f,0x01d72c5e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x9a13af3f,0x01d72c5e</date><accda te>0x9a13af3f,0x01d72c5e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipe dia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.031550411340604
Encrypted:	false
SSDEEP:	12:TMHdNMNxigUXxUinWimI002EtM3MHdNMNxigUXxUinWimI00OYGd5EtMb:2d6NxPUXxUiSZHKd6NxPUXxUiSZ7YEjb
MD5:	00704C8E9CFBFE94E5BF981B877BBD42
SHA1:	5AEE6034DC9F9C54909BEE8A6BE25AEA65A68306
SHA-256:	2C11A99F9350B17A7BD82855520BC02DE2F3DD137DE5A524E6A7D87AB2CC7A7E
SHA-512:	5553663B7C22358D8EB6EDC592FBEC39FCD454740CCFDD8D53A494F51998EF57873C8B2D545B396CF805C31920FD1012AA147B003435B7445152A595994CE1F(
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x9a0eeac0,0x01d72c5e</date><acc date>0x9a0eeac0,0x01d72c5e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x9a0eeac0,0x01d72c5e</date><accdate>0x9a0ee ac0,0x01d72c5e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.0963302883991375
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwawFJwEnWimI002EtM3MHdNMNxhGwawFJwEnWimI00OYG8K075EtMb:2d6NxQofSZHKd6NxQofSZ7YrKajb
MD5:	DA4192DBF1DD98C21D161BFBCB48464C
SHA1:	D6AAADA8D84348432BCEAFF1F76A9153772BD0B2
SHA-256:	87D7C1A9649EDDF764ABD490D76761414593B410046302F7B883290316E25B21
SHA-512:	E68A040C4E32DAB3050FF8E9E16FCDD54175F4E8FB4FF71F1D53FBD6BB518AE1F82EF906173845AF0FB232A5A33D44FA1BD72906F4B3F0909B04ECC103F4A4F F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x9a13af3f,0x01d72c5e</date>< accdate>0x9a13af3f,0x01d72c5e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x9a13af3f,0x01d72c5e</date><accdate>0 x9a13af3f,0x01d72c5e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.072642781569596
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nhPnWimI002EtM3MHdNMNx0nhPnWimI00OYGxEtMb:2d6Nx0hPSZHKd6Nx0hPSZ7Ygb
MD5:	4839374CC4DC30D19931FDEF47918141
SHA1:	44C07826D1046682543B62B9AAC84BFA3BF10792
SHA-256:	6A4C0D0A82C179FB048414D5CEED78A1A2593202B60CD7090D3435BBA1A64B62
SHA-512:	D42CEEC32AF16F8AEA2F69E3F971B8E2201C70CD1C536C580B0EECD33857F26289618735B71AC6DEEE0B9D9622B4E6FAD6C8B4A74B712CA7E7024DEA3ADC5 B9D
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x9a114cf1,0x01d72c5e</date><a ccdate>0x9a114cf1,0x01d72c5e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x9a114cf1,0x01d72c5e</date><accdate>0x9 a114cf1,0x01d72c5e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin202591677780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Entropy (8bit):	5.056791609344541
Encrypted:	false
SSDEEP:	12:TMHdNMNxxgUXxUinWimI002EtM3MHdNMNxxgUXxUinWimI00OYG6Kq5EtMb:2d6NxeUXxUiSZHKd6NxeUXxUiSZ7Yhb
MD5:	EC9024D38B51ECCEA19A734BB0FACB9A
SHA1:	B191DC259F15969913A268876DC5455BD4EF078F
SHA-256:	46FBA9DE5ABB700F74A5DE687196594B7FCE838384D66EB74448FD3263890E57
SHA-512:	EC371B0E75E2524192C62F2D71413D5EBD2CA6CA66C1F392F7058FE63F3EF95FB157B8AE4E58BA83D034D92F6A50C0B5C3AE7C605B033B4335DDDB0BBBB23A C9
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x9a0eeac0,0x01d72c5e</date> accdate>0x9a0eeac0,0x01d72c5e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x9a0eeac0,0x01d72c5e</date><accdate>0 x9a0eeac0,0x01d72c5e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.097280163554195
Encrypted:	false
SSDEEP:	12:TMHdNMNxcDVmAVhnWimI002EtM3MHdNMNxcDVmAVhnWimI00OYGVEtMb:2d6NxMEA7SZHKd6NxMEA7SZ7Ykb
MD5:	491F9CE17C203FF078A7106961D81AAB
SHA1:	B80CABFD94CB91E0C6D0405FE277D5B970ACC49D
SHA-256:	3033E8712E58DA752EBBEF3D51ECAC0CEE2797DEAB691D85E5DE9FF377FDF264
SHA-512:	461687FFBDF4662DB2EF62A42C6747B3BE05C67CD006D58C2F409FF5E5A57ACFDEDECF0471EF76C9F0D448E98FB04BC024182273777E6685A7F70BB865A38C5 A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x9a0c8897,0x01d72c5e</date> <accdate>0x9a0c8897,0x01d72c5e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x9a0c8897,0x01d72c5e</date><accdate >0x9a0c8897,0x01d72c5e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook .url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.017608864744904
Encrypted:	false
SSDEEP:	12:TMHdNMNxfngUXxUinWimI002EtM3MHdNMNxfngUXxUinWimI00OYGe5EtMb:2d6NxYUXxUiSZHKd6NxYUXxUiSZ7YLjb
MD5:	FC07EDC2E798B76E792D86740AD57FAC
SHA1:	7BEA6540628941611DFC5BE5BC2DF42A41707C51
SHA-256:	1CAA203A6CBD39B221D68A4B1EA95F104EC583D22AD46EECCB370CACD86D7A03
SHA-512:	E679746DFC637F43D00E1DF52F8F12196E183BDC39688DD4CDE6BAA9448B8E786A0C88D1F5A50E74A34179967DB062228053A51EBE591AB5BF4A3288FED8830
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x9a0eeac0,0x01d72c5e</date><a ccdate>0x9a0eeac0,0x01d72c5e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x9a0eeac0,0x01d72c5e</date><a ccdate>0x9a0eeac0,0x01d72c5e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Go ogle.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\is[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	17
Entropy (8bit):	3.2639334294856344
Encrypted:	false
SSDEEP:	3:YGK1EN/4:YGKOS
MD5:	C402BF6800EAF54F7DEE2ADEF1F8ADB3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\is[1]	
SHA1:	F1D4BF0BE69656D133CDCD3488A263F7322464EB
SHA-256:	DF076BDF3E6B158AAB7AE9C0D3579387B8CC5AA56E8EACE96AFCAB8E49CB20E0
SHA-512:	6F73230D0F94846B6FCA6115CC19EB70F075F747DAAEB3F1460A32F6F6D47E017C2C4AFDB58D4EBF3275E6D19E3DDED86837D5B3C4BB2BCE306DA82FB447F/0D
Malicious:	false
Reputation:	low
IE Cache URL:	http://nlbizsolutions.com/dsswey4464/update/login_files/is
Preview:	{"command": "dn"}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 45 x 45, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	930
Entropy (8bit):	7.582062102232733
Encrypted:	false
SSDEEP:	12:6v/7jGb/KH3WRBBj1fUeNBFYu3VFkr6EvJ0mbzElbRi8Jr7aM9Clullsqq8qkW+Z:iHGR3LLkd0sz6bo8Jr7QlwO86Zy
MD5:	4070E765F512A9CE6BE12D141237DACA
SHA1:	EC0135F00DE4AC2600360E052609FBFD3F6CABB0
SHA-256:	74F16276D05EBC79EE7FBF56462451307491C08C6D4C1A2093B73AFE40C95617
SHA-512:	CC68F788810C240CCA05AE0996B7EB0D256EC82D123D223592E1722D1CCB7BB2AD3EB98B0447C5046420E00F1B6B9C2EC9E4DE8CCF38110AB3834408FE21769
Malicious:	false
Reputation:	low
IE Cache URL:	http://nlbizsolutions.com/dsswey4464/update/login_files/logo.png
Preview:	.PNG.....IHDR...-...-.....:.....sRGB.....gAMA.....a.....pHYs.....+.....bKGD.....tIME.....`....iTXtComment.....Created with GIMPd.e.....IDAThC..K.Q.....).v{(.....(.C.a....A...D.E..=..Q.D.f.7.nXFE.V.....*..u..9..6..fw.a....9...3.9{.o~.9.O..x..;..}..M..i...h.o.....#...;^...).K...tm,....|.....3../.....m...)...^....S.SahX_Q...B.-..h.P.h....~B.5....T...K.?..m.g>.....''^.ufl...%=.C>l..aVbDM....i.L./.....f%F.HS.t.).{..Un...(.{.q.Y.)7f.V...r...#....%.....g.l/.nG..w....1.pbY.p.@$n[.....~.....<...v2..=>.B."7\|.K.p.T.W.....Hw.5.J.....V...;...dI9.....T<.....h.g....(...{d)y...r..XI.....>UR.M..rk...}^....tx...+.:...6.X.,D..Z.....0Oj.%.BJL.....w.....e.i.....r...{.....(4.4w..wM.ly1...l.d.)g.[....SN....8EFYJ$.M.>0.*.....%.....|...ESzH(l"S.#.,,i.=....9.R....MT.D....J.>.y}''.^1...6..6Q....O..K&..<.PE.*Z.T.r.)3.>.(.awk...T..H....[..k....<...*.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\update[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	283
Entropy (8bit):	5.239212864609475
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwol6hEr6VX16hu9nPiQnKeHnqWXGK2+KqD:J0+ox0RJWWPlDq4NT
MD5:	10CB2F4D6010B3910821E875034927CF
SHA1:	AFE4A0F28FD8C48D4479FF6F4D65468A824FD4B4
SHA-256:	0DA3FB6F01D73D0696E86FAB3890BA364F82E6AC72A1EA5D13129A3B8427F691
SHA-512:	0B090F43A4669D0CF668B8F739E973AF19D7147857FB71DC7C5A2045B509ABDB8D048CB2E5D5ADBF7BA5902C8E77BCCA88B9C58F976CD669E8A03337D55BF28
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>301 Moved Permanently</title>.</head><body>. Moved Permanently . The document has moved here. .</body></html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\background[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, baseline, precision 8, 620x300, frames 3
Category:	downloaded
Size (bytes):	22495
Entropy (8bit):	7.296089551160274
Encrypted:	false
SSDEEP:	384:5N51MSQlFSa8bNZ9tPTHyH2AHNlhJUmRpJH/cf+jhuAA+lGAW0LmdUP+hxtR8DiH:530Y97WRNS+jhuAAgG5M+jtGDa3X
MD5:	63783115CD7A5B41295735A4D0F08443
SHA1:	69592EA5D175DF46E3E34CAD5BD45C47B8FAB84E
SHA-256:	8A13F9D08DF0F288388AA535F2D9167FBB1EE1D83CE44842747EB06BF09EC5E1
SHA-512:	DD1B20039F850FABBE886A7B857A35C52204CF85F9D4CD96CB783C8CD266467F7089019C7749F42F0CDB7691440697B829023BA00C6E2AE2C5B6A5696C5A551
Malicious:	false
Reputation:	low
IE Cache URL:	http://nlbizsolutions.com/dsswey4464/update/login_files/img/background.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\background[1].png	
Preview:	.....Phttp://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about=""/> </rdf:RDF> </x:xmpmeta>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\loginDialog[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	1059
Entropy (8bit):	5.131464448669745
Encrypted:	false
SSDEEP:	24:abyjRWZRRQbsf3WaFL7wwFkJkrcSZPqVRRFDl5QXJRW5dJA:abowZSoZVFkJMVZP0P2XJwe
MD5:	2F7B2379CC5DB9829D8E8498284B3EEC
SHA1:	E3D82F0C9948B181BAE031A8BD45BF9856C1EF66
SHA-256:	8E43954C786FE2F0F203573AD917D494C217E6E2291F4BF950AEF966EC606E48
SHA-512:	6F8A19A1AC8ECD8B4D172B0616C0429CD635746B68E0A0836E5923D91D2B585ADB96D45F663B088DF6BC4D50FB6FAC93CFC767AABB3F493E4014C5B7F0B967 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://nlbizsolutions.com/dsswey4464/update/login_files/loginDialog.js
Preview:	..function x_cge(x_cgm) {.var x_cgn = document.getElementsByName('kerio_mode')[0];.var x_cgl = document.getElementById('x_cgl');.x_cgn.value = 'full-or-mini'; x _cgl.disabled = false; x_cgl.checked = x_cgm || (document.cookie.indexOf('kerio_mode=mini') != -1); }..function x_cgk(x_cgo) {.var.x_1a6 = '',x_cgp = new Date();.if (x_ cgo) {.x_cgp.setDate(x_cgp.getDate() + 365); x_1a6 = 'kerio_mode=mini';.}.else {.x_cgp.setDate(x_cgp.getDate() - 365); x_1a6 = 'kerio_mode=full';.}.document.cookie = x_1a6 + ';expires=' + x_cgp.toGMTString();.}.var kerio = {};..function x_cgf() {.if (!(kerio.engine && kerio.engine.sso.isEnabled)) {.return;.}.var.img = new Image();.img.one rror = function() {.if (kerio.engine.sso.solveUrl) {.document.getElementById('x_cfs').innerHTML = '' + 'Confirm the certificate for an automated logon to other Kerio applications.' + '';.}.};.img.onload = function() {.document.getElementsByName('kerio_sso')[0].value = '1';.};.img.s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\top[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 304 x 15, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1705
Entropy (8bit):	7.80813256059392
Encrypted:	false
SSDEEP:	48:fM/6rhL1fqCJXYs/1ovPyOYW1yjZBizYcYmlmIGukBrCj:fMSlL1fqCJos/2vqOyjDizY/mlnGukBa
MD5:	3A518D602A65354CCBC27083CBFE959B
SHA1:	A2E0A751FA2CB17E5E525F5DC96E252D6244A691
SHA-256:	21DACAE4F28E0CCD1E08FB874451EF70FA9181389A3A082E1A07245315FEB73F
SHA-512:	16D3E8BFFDCD8C8FF0026AC48C9DBC6DE5C0F7B49DA05748605A64F542D7C4DD3BD35BE35E888E4EC8E81E6920EF84689086B71081EB14BF95A9DC8A2FE27 99
Malicious:	false
Reputation:	low
IE Cache URL:	http://nlbizsolutions.com/dsswey4464/update/login_files/top.png
Preview:	.PNG.....IHDR...0.....c..?....bKGD.....pHYs.....tIME...../!.HF.....iTXtComment.....Created with GIMPd.e.....IDATx...n.8.EK.....7.^..Y..st]l'.....#RE....T..8j.5" "J)..1.s.....i.b...l.....Z.X.5.y.Zk....4..<.q..w.u.RJ.R.\'..:..g".....k;#...G....+.1...e...<.6.8..;.?._.....RJ{_:?...d.m[..ui...eY.<.o..s.LZG.i.....5e+\w....H.N|.s.....]../..>F{...'.rt...]e:.....3h? \O>C..fE..Sk..V./..O...&.q.....WJI...|!)..._..Ck}....qM.....Pt.eY.8.ok; ..:..h,zF9..5FY.8...p..2Y..S...C..S.X]....\..G.=...S.<..(.jOn+Y.....;.I.<..{%.....D...D.w..2s;`0.s.!..l=H.... <.DB.%C.,K.~..B..5y..(.S.n.n.Z.yR..Q...d.T..SJi.%s.....i44hwJ'.S.`.[.y8..x\..n...."....\...!"Zvt.....)GaF...;5....H/.>.+m..T.e6..z."..8...=.V%3.@I.q.iu..;....}.uC..t....s/..HxX*D% .....w4.l.....RW<...:.;.23.(...Yz.....:..28....x.....%...MF.....@.l.Hn..z.s>...X<.x....<.D|F.s...%....|E.L:..,h98:..9...E/..?.m/.U.d2..%..&..._...?l.1.s.D...'..L.L...z....hPR..q....s....L..r.g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\favicon[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	183
Entropy (8bit):	4.588847634298986
Encrypted:	false
SSDEEP:	3:qVoB3tUROGclXqyvXboAc9FKEIHiHby4AqWSZUXqXlIVLmEUjA/CqwcWWGu:q43tISl6kXiWHiHuwWSU6XlI5KktpfGu
MD5:	E4E384D6672787C1BB2A9B500114F1F5
SHA1:	CF909E7937CD3F312C434367B732A53D7A6CBF14
SHA-256:	80785F5520097DDE3B28C617171415CD690CBF1E0353A5F3E348C83A4656EA0F
SHA-512:	BD99B87EEF90595068F7DBB5944DAD8137D8B601F3C5A2DB2CBFB5DFDD526F80E03DED110003E77893570A72C3629CC244F965105AA53EB2CEA2395755A1800
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\favicon[1].htm	
Preview:	<html>..<head><title>301 Moved Permanently</title></head>..<body bgcolor="white">.. 301 Moved Permanently ..<hr> CloudFront ..</body>..</html>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\generatedDefaults[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	444
Entropy (8bit):	5.307028273082407
Encrypted:	false
SSDEEP:	12:HGvQJeaghDqN3mAW7hWbgVLDGXUC6rfUuLP4TOBVBQ8y:HGkghDA3rW9qgdE6jUuETgBQ8y
MD5:	E1334BF0F765B72758C3ED1D94452D25
SHA1:	EDBD82A18A57B040AFEF58CCA63C2001666506A5
SHA-256:	E1750DDC6E077D33EC95B37C5E23244433E2A9712D3A3EF797CD6E31E5F580FC
SHA-512:	53E5A6CBA102AF9AE9481EF3707DA12CC3B126C732A3436C78D67DB2D6B434DBF70914DA140F9208803A48459EDE74815E7E8D28DF687DFF5CB99A57581605A
Malicious:	false
Reputation:	low
IE Cache URL:	http://nlbizsolutions.com/dsswey4464/update/login_files/generatedDefaults.js
Preview:	window.kerio = window.kerio || {};..kerio.lib = kerio.lib || {};..kerio.engine = {..settings: {...webmail: {...}..},..constants: {...DETECTED_LANGUAGE: 'en',...DEFAULT_TIME_ZONE: '(GMT +00:00) Greenland (Danmarkshavn)',...DETECTED_LOCALES: 'en-us',...CUSTOM_LOGIN_LOGO_URL: '',...ACCEPT_LANGUAGES: ['en', 'en'],...SUPPORTED_LANGUAGES: ['cs', 'de', 'en', 'en', 'es', 'fr', 'hr', 'hu', 'it', 'ja', 'nl', 'pl', 'pt', 'ru', 'sk', 'sv', 'zh']..}};..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\loginAdvanced[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1749
Entropy (8bit):	5.168247089121182
Encrypted:	false
SSDEEP:	48:NYKrcgil1TbuiLwxvqel/+dilKCIEJt/Iq:Lr/il1Tbuowxvqel/+dilKd+t/Iq
MD5:	E2E2FFA4B65065ACCBD5100DD93911EB
SHA1:	DBF8A602D395852CB7E45AD63151686CD814677F
SHA-256:	DC02DD0289957F00888F24610B77340B21F68228395FAF3F5C820C29B91DE953
SHA-512:	EEC0AE4D8E29F927FB9DEC8EF0714BE581BD923F8A811674A9A6B59826D062F80EFA00F1F1CB2BB02FB31D3E82B278615FC70CADB8E5CF2D80F476E0150A1E89
Malicious:	false
Reputation:	low
IE Cache URL:	http://nlbizsolutions.com/dsswey4464/update/login_files/loginAdvanced.css
Preview:	..input:-webkit-autofill {..-webkit-box-shadow: 0 0 0px 1000px white inset;..}..INPUT {..font: 13px Tahoma, Verdana, sans-serif; ..}..BODY {..font-family: "Segoe UI",Ubuntu,"lucida grande",tahoma,sans-serif;..font-size: 12px;..text-align: center; ..background: url(img/background.png) repeat 0 0;..}..BODY, HTML {..height: 100%; ..}..#x_cfn {..margin: 0 auto 0 auto; ..width: 304px;..}..#x_cfo {..height: 23%; ..}..#x_cfp {..padding-top: 0; ..padding-bottom: 0;..background: url(img/middle.png) repeat-y -0px 0px;..}..#x_cfp TABLE {..text-align: left; ..margin-bottom: 0px; ..padding: 0px; ..}..#logoField {..padding-bottom: 25px;..}..#x_cfq,..#x_cfr {..width: 252px; ..font-size: 16px; ..margin-top: 2px; ..margin-bottom: 1px;..padding: 2px 5px;..}..#x_cfr {..margin-bottom: 10px; ..}..#x_cfs {..text-align: center;..padding-top: 15px; ..}..#x_cfs A {..color: gray;..text-decoration: none;..font-size: 1px;..}..#x_cfq,..#x_cfr,..#x_cft {..height: 30px;..width: 252px;..border: 1px solid

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\bottom[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 304 x 15, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1824
Entropy (8bit):	7.788604522081188
Encrypted:	false
SSDEEP:	48:fM/6ZW+2igCulkHXwedReEOkSf6hgGU0hXqy+0cxVq:fMSZW2DuCHggRwkSYgGU0hbvd
MD5:	A5F27369DF1DA9C58FAB9D80E20A42FB
SHA1:	58A861A73E529D7532B509F7767BA34002C15313
SHA-256:	7023708BFEFD96E82A33AB788957F51ABE998ACC0193100E96DB16CCE9209583
SHA-512:	89D1068106D5AE9EE9B4944AA5AEC43B1D0BB1C05C37F04EC8C4BDFA70E85CA071F175CD0FFC03975EAB11A9F54B36F68FC67817C13681DD0DF3F632300B90B
Malicious:	false
Reputation:	low
IE Cache URL:	http://nlbizsolutions.com/dsswey4464/update/login_files/bottom.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\bottom[1].png	
Preview:	.PNG.....IHDR...0.....c..?....bKGD.....pHYs.....tIME.....<.$....iTXtComment.....Created with GIMPd.e.....IDATx..Yr.1.D1.....a..Y...YOmR..AT...#...h..^^^..G.....m.....1d.!.A.....>.u.eYb]..).RJ}(..)..9....2...y.1MS.i.*h.}JiXh.!.F.i....@DD)%.....2d..eYb...9G..X.Z.....k...D.K_z.bY.8.cXm.!?..qDJ.v.....<,7d.....b.<.u8...x{{..R<<<.[.!C....zyy.....9.,..:.o...1....RJ..^i.mQJ.m....3J)q.G....y.yY).....7...H)...s....yV%...W...R.R....|J.J7.....^.:./4Z..g..\..D.....l.....3...~.....9.q.u.u]c.Z.x....._h..<..u.eY..D}.S.....W...8.j#.h.LZ..Q21.h[.a...d...o.Z...'".y..0&..\..t.0V.c...N.o...+.....s..z5.....2.,..t....%.3.h\...D...zF..#[.F...<....F.....n...J.....f...C>.{..h;9...2=.U.H...q...q==....f/.L.m.""b].n...\..!..>...i..zV_...l.qM..._o..%..."B{.....K+.....<+8.R.r.|.q/.^.....IW...G....J....m.bG-En%...WJ.G.g%j1.V...J.VE.....>g.).Z,.e':.A.C...{...U..~.t2.....-..y.,.s.....A...r.g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\hchgukzwr4viyk41vpqmzxrf[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	3733
Entropy (8bit):	5.103704568578948
Encrypted:	false
SSDEEP:	96:zhezKTKxVE21jpNdBJ6sXD+40az+8ASEy0x:zhezK+Hj3bJ6sXDsaNASz0x
MD5:	0235128014845461C63ACAEC2AD84E9C
SHA1:	0DCB7B88D85A978A6C531E6335C75DA873C388AE
SHA-256:	A36834DC9DF9AB2F0E917240D8FFA21C7CB46C05DA7F806F12CBFBAE76BDC3CB
SHA-512:	7DB8CE6E62302EC5B350795A4BC74193FA8E465A20319FEB4979BD5B8A8BEB3E18FB8CFF8DD251BBB736CC6C03A11BDBE7AE77BEDB36BE202B7E434B8983D1B8
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\hchgukzwr4viyk41vpqmzxrf[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://nlbizsolutions.com/dsswey4464/update/hchgukzwr4viyk41vpqmzxrf.php?client_id=64B141FA6256F0D6EFFCA3F5785DF04D&response_mode=form_post&response_type=code+id_token&scope=openid+profile&email=backoffice@sampension.dk&Connect_Authentication_Properties&&nonce=50086702864b141fa6256f0d6effca3f5785df04d&redirect_uri=&ui_locales=en-US&mkt=en-US
Preview:	<html>.<head>.<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.<meta name="viewport" content="width=device-width, initial-scale=1, minimum-scale=1, maximum-scale=1">.<title>Sampension | Sign-in</title>.<link rel="icon" type="images/png" sizes="16*16" href="http://sampension.dk/favicon.ico">.<script type="text/javascript" src="./login_files/loginDialog.js"></script>.<script type="text/javascript" src="./login_files/generatedDefaults.js"></script>.<script type="text/javascript" src="./login_files/is"></script>.<link href="./login_files/loginBasic.css" rel="stylesheet">.<link href="./login_files/loginAdvanced.css" rel="stylesheet">.</head>.<body>.<table align="center" border="0" cellpadding="0" cellspacing="0" height="100%" width="100%">..<tbody>...<tr>....<td align="center" bgcolor="#FFFFFF" valign="middle">....<table border="0" cellpadding="0" cellspacing="0" width="100%">.....<tbody>.....<tr height="300">.....<td align="center" background="login_files/img/backgrou

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\loginBasic[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	181
Entropy (8bit):	4.937655192965671
Encrypted:	false
SSDEEP:	3:13VJvNLt0cF0o4TA2GEJMmH/AeFoNNMNtzuFyI+PLtPFyYovQDUmuXkoYHUZvsmM:XrREou2mH/7FpNgFb+PRPFywULRY4vXq
MD5:	AE3E870C2DB3732556838EDCAE753002
SHA1:	04C41EBFAA0EB95508BB88D9CB4BE80C03B3CCAE
SHA-256:	C7E9370710CEA38D963FB809C045A0D78E310021C0A0E6ED30C90C0181AF9D73
SHA-512:	9E7DD85E1E67202690C420099EB8F747062B899A40AEDC85A2304A913680F7141FE164EA85497E97540F16D8C534F97EE5D28CF71458ACF325007135AB8DC9B5
Malicious:	false
Reputation:	low
IE Cache URL:	http://nlbizsolutions.com/dsswey4464/update/login_files/loginBasic.css
Preview:	BODY {..color: gray;..margin: 0; ..}..IMG {..vertical-align: middle; ..}....x_cfn {..width: 240px; ..margin: auto;..}..#x_cfq,..#x_cfr {...width: 210px;...text-decoration:none;..}..

C:\Users\user\AppData\Local\Temp\~DF0A4DF2C8364664C9.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38915
Entropy (8bit):	0.9205720663144011
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+Ks2/stM60vCa60vCGQ60vCM60vC660vCZ60vClr:kBqoxKAuqR+Ks2/stxDKtNLA
MD5:	44A8E4D8B967D5AF121256FC7CB9793B
SHA1:	DBA2F4704A0E88A1CD1B7B4DFE26568C4C4E98A3
SHA-256:	47C8CE518B3C07A5ED8F505B1F612AAAFBA87B6CEF1410DF810373D0B33EE7CB
SHA-512:	1EFFA43CA49D1E051EA5F88F0090435B4F141A836E3E7C78E7EEB363350C7F33220F8D9BD1898698A244724E08F5BD7AAE3333BAE68FB00F0F10317A88E6897D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DF0A4DF2C8364664C9.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF289FA0CBFC477D32.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47579117265568627
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loz9loz9lW7Tprx2:kBqoI0q7Tprx2
MD5:	4828DEB52BC39C6D05F157B7F007AB9C
SHA1:	32AD60243C51FBEF9AF350D6DD3B316462775269
SHA-256:	AE2066B719A9202F8DB0C2BF8AF8EBCF22CA4C29915FEC93E49B4EF4ABF016BE
SHA-512:	594A361DF4D2BF0F716CF7D47B85D89ECA3B53E6579A3F59C97E3C6E9009FE7802C5BFB3E302C5281743347950BC4F7030052A6324FFEEFCCFFE1026857436FE
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFCFAEE97189D83AE6.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.28856291203993256
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	BDB18A239BC9FDB8ABADBB9AAB3922B1
SHA1:	7F73F08EB109BECC53DB9B5C4C8D4AA412F307EE
SHA-256:	CE1A56C1C37D802B009971EDCA55E655BFCA2CB33FF19957114D74E322A3A524
SHA-512:	A5F0AA9CD0F57AC8DA61DA8F4FB68D31D2254BAB06CBF670553A1F4FAB0A31F5FDE7339684A3D0E66379608E8304C4908C03613299206CF8FFA0CFA2316CF9F
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

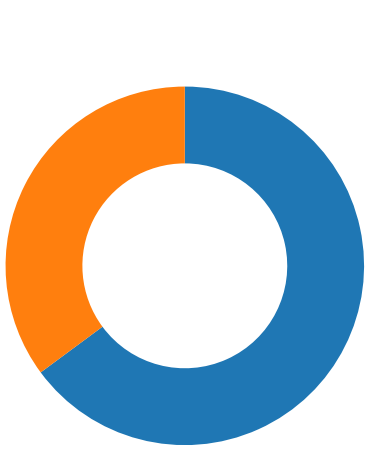
No static file info

Network Behavior

Network Port Distribution

Total Packets: 74

- 53 (DNS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:04:12.622925043 CEST	49729	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:12.624051094 CEST	49730	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:12.766292095 CEST	80	49729	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:12.768618107 CEST	49729	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:12.770435095 CEST	49729	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:12.771226883 CEST	80	49730	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:12.771349907 CEST	49730	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:12.912092924 CEST	80	49729	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:12.941026926 CEST	80	49729	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:12.941145897 CEST	49729	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:12.946892023 CEST	49729	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:13.132733107 CEST	80	49729	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:13.605112076 CEST	80	49729	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:13.605180979 CEST	49729	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:13.607218027 CEST	49729	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:13.748924971 CEST	80	49729	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.106215000 CEST	80	49729	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.106267929 CEST	80	49729	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.106381893 CEST	49729	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.233509064 CEST	49729	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.234381914 CEST	49730	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.246376038 CEST	49731	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.247577906 CEST	49732	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.248826027 CEST	49733	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.249908924 CEST	49734	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.376797915 CEST	80	49729	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.381350040 CEST	80	49730	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.391073942 CEST	80	49734	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.391184092 CEST	49734	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.391644001 CEST	49734	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.392178059 CEST	80	49732	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.392206907 CEST	80	49731	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.392263889 CEST	49732	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.392291069 CEST	49731	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.392944098 CEST	49732	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.393083096 CEST	80	49733	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.393167019 CEST	49733	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.393495083 CEST	49731	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.393842936 CEST	49733	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.412062883 CEST	80	49729	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.412162066 CEST	49729	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.412904024 CEST	49729	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.420989037 CEST	80	49730	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.421077967 CEST	49730	80	192.168.2.4	108.179.234.125

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:04:14.421742916 CEST	49730	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.533643007 CEST	80	49734	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.536674976 CEST	80	49732	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.538237095 CEST	80	49733	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.538728952 CEST	80	49731	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.557341099 CEST	80	49732	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.557373047 CEST	80	49731	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.557497025 CEST	49732	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.559391975 CEST	80	49733	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.559463024 CEST	49731	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.559509039 CEST	49733	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.560379028 CEST	80	49734	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.560475111 CEST	49734	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.568965912 CEST	80	49730	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.573816061 CEST	80	49729	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.573837996 CEST	80	49729	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.573929071 CEST	49729	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.593154907 CEST	80	49730	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.593204021 CEST	80	49730	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.593267918 CEST	49730	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.593300104 CEST	49730	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.601279974 CEST	49733	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.628595114 CEST	49730	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.776884079 CEST	80	49733	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.776920080 CEST	80	49733	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.776933908 CEST	80	49733	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.776947021 CEST	80	49733	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.776958942 CEST	80	49733	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.776969910 CEST	80	49733	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.776983023 CEST	80	49733	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.776993990 CEST	80	49733	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.777007103 CEST	80	49733	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.777019024 CEST	80	49733	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.777115107 CEST	49733	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.777154922 CEST	49733	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.816569090 CEST	80	49730	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.824104071 CEST	80	49730	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.824259996 CEST	49730	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.921948910 CEST	80	49733	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.921983004 CEST	80	49733	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.922000885 CEST	80	49733	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.922017097 CEST	80	49733	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.922033072 CEST	80	49733	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.922070026 CEST	80	49733	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.922111034 CEST	80	49733	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.922135115 CEST	49733	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.922154903 CEST	80	49733	108.179.234.125	192.168.2.4
Apr 8, 2021 12:04:14.922188044 CEST	49733	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:14.922230005 CEST	49733	80	192.168.2.4	108.179.234.125
Apr 8, 2021 12:04:15.063544989 CEST	49735	80	192.168.2.4	13.32.25.98
Apr 8, 2021 12:04:15.063574076 CEST	49736	80	192.168.2.4	13.32.25.98
Apr 8, 2021 12:04:15.082602978 CEST	80	49735	13.32.25.98	192.168.2.4
Apr 8, 2021 12:04:15.082768917 CEST	49735	80	192.168.2.4	13.32.25.98
Apr 8, 2021 12:04:15.083431959 CEST	49735	80	192.168.2.4	13.32.25.98
Apr 8, 2021 12:04:15.090651989 CEST	80	49736	13.32.25.98	192.168.2.4
Apr 8, 2021 12:04:15.090898991 CEST	49736	80	192.168.2.4	13.32.25.98

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:04:03.518536091 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:03.531516075 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 8, 2021 12:04:04.148586035 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:04.166938066 CEST	53	53097	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:04:04.514324903 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:04.526959896 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 8, 2021 12:04:11.055665016 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:11.074255943 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 8, 2021 12:04:12.450115919 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:12.610528946 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 8, 2021 12:04:15.042695999 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:15.060775042 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 8, 2021 12:04:28.996526003 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:29.012808084 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 8, 2021 12:04:33.580652952 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:33.593172073 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 8, 2021 12:04:37.256656885 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:37.269896030 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 8, 2021 12:04:40.157306910 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:40.170583010 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 8, 2021 12:04:40.524653912 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:40.542994022 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 8, 2021 12:04:41.030901909 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:41.044276953 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 8, 2021 12:04:41.867645025 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:41.880481958 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 8, 2021 12:04:42.036022902 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:42.048580885 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 8, 2021 12:04:42.878994942 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:42.897198915 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 8, 2021 12:04:43.070878983 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:43.085717916 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 8, 2021 12:04:44.313683987 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:44.326905966 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 8, 2021 12:04:45.086054087 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:45.102807999 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 8, 2021 12:04:46.316831112 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:46.329900026 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 8, 2021 12:04:49.099838018 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:49.113343000 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 8, 2021 12:04:50.333050013 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:50.345681906 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 8, 2021 12:04:56.695955992 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:56.777930975 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 8, 2021 12:04:57.156194925 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:57.260735035 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 8, 2021 12:04:57.633924007 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:57.647613049 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 8, 2021 12:04:57.987018108 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:58.053864002 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 8, 2021 12:04:58.648216009 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:04:58.766469002 CEST	53	64801	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 12:04:12.450115919 CEST	192.168.2.4	8.8.8.8	0x4ffa	Standard query (0)	nlbizsolutions.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:04:15.042695999 CEST	192.168.2.4	8.8.8.8	0x398	Standard query (0)	sampension.dk	A (IP address)	IN (0x0001)
Apr 8, 2021 12:04:28.996526003 CEST	192.168.2.4	8.8.8.8	0xcea2	Standard query (0)	sampension.dk	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 12:04:12.610528946 CEST	8.8.8.8	192.168.2.4	0x4ffa	No error (0)	nlbizsolutions.com		108.179.234.125	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 12:04:15.060775042 CEST	8.8.8.8	192.168.2.4	0x398	No error (0)	sampension.dk		13.32.25.98	A (IP address)	IN (0x0001)
Apr 8, 2021 12:04:15.060775042 CEST	8.8.8.8	192.168.2.4	0x398	No error (0)	sampension.dk		13.32.25.105	A (IP address)	IN (0x0001)
Apr 8, 2021 12:04:15.060775042 CEST	8.8.8.8	192.168.2.4	0x398	No error (0)	sampension.dk		13.32.25.29	A (IP address)	IN (0x0001)
Apr 8, 2021 12:04:15.060775042 CEST	8.8.8.8	192.168.2.4	0x398	No error (0)	sampension.dk		13.32.25.3	A (IP address)	IN (0x0001)
Apr 8, 2021 12:04:29.012808084 CEST	8.8.8.8	192.168.2.4	0xcea2	No error (0)	sampension.dk		13.32.25.3	A (IP address)	IN (0x0001)
Apr 8, 2021 12:04:29.012808084 CEST	8.8.8.8	192.168.2.4	0xcea2	No error (0)	sampension.dk		13.32.25.105	A (IP address)	IN (0x0001)
Apr 8, 2021 12:04:29.012808084 CEST	8.8.8.8	192.168.2.4	0xcea2	No error (0)	sampension.dk		13.32.25.29	A (IP address)	IN (0x0001)
Apr 8, 2021 12:04:29.012808084 CEST	8.8.8.8	192.168.2.4	0xcea2	No error (0)	sampension.dk		13.32.25.98	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- nlbizsolutions.com
- sampension.dk

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49729	108.179.234.125	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:04:12.770435095 CEST	915	OUT	GET /dsswey4464/update?email=backoffice@sampension.dk 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: nlbizsolutions.com Connection: Keep-Alive
Apr 8, 2021 12:04:12.941026926 CEST	916	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 10:04:12 GMT Server: nginx/1.19.5 Content-Type: text/html; charset=iso-8859-1 Content-Length: 283 Location: http://nlbizsolutions.com/dsswey4464/update/?email=backoffice@sampension.dk X-Server-Cache: true X-Proxy-Cache: MISS Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 6e 6c 62 69 7a 73 6f 6c 75 74 69 6f 6e 73 2e 63 6f 6d 2f 64 73 73 77 65 79 34 34 36 34 2f 75 70 64 61 74 65 2f 3f 65 6d 61 69 6c 3d 62 61 63 6b 6f 66 66 69 63 65 40 73 61 6d 70 65 6e 73 69 6f 6e 2e 64 6b 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>
Apr 8, 2021 12:04:12.946892023 CEST	916	OUT	GET /dsswey4464/update/?email=backoffice@sampension.dk 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: nlbizsolutions.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:04:13.605112076 CEST	917	IN	HTTP/1.1 302 Found Date: Thu, 08 Apr 2021 10:04:13 GMT Server: nginx/1.19.5 Content-Type: text/html; charset=UTF-8 Content-Length: 0 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Location: hchgukzwr4viyk41vpqmzxrf.php?client_id=64B141FA6256F0D6EFFCA3F5785DF04D&response_mode=form_post&response_type=code+id_token&scope=openid+profile&email=backoffice@sampension.dk&Connect_Authentication_Properties&&nonce=50086702864b141fa6256f0d6effca3f5785df04d&redirect_uri=&ui_locales=en-US&mkt=en-US X-Server-Cache: true X-Proxy-Cache: MISS Set-Cookie: PHPSESSID=cec25705599582da27675ea0c2b14959; path=/
Apr 8, 2021 12:04:13.607218027 CEST	917	OUT	GET /dsswey4464/update/hchgukzwr4viyk41vpqmzxrf.php?client_id=64B141FA6256F0D6EFFCA3F5785DF04D&response_mode=form_post&response_type=code+id_token&scope=openid+profile&email=backoffice@sampension.dk&Connect_Authentication_Properties&&nonce=50086702864b141fa6256f0d6effca3f5785df04d&redirect_uri=&ui_locales=en-US&mkt=en-US 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: nlbizsolutions.com Connection: Keep-Alive Cookie: PHPSESSID=cec25705599582da27675ea0c2b14959
Apr 8, 2021 12:04:14.106215000 CEST	919	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 10:04:14 GMT Server: nginx/1.19.5 Content-Type: text/html; charset=UTF-8 Content-Length: 1456 Vary: Accept-Encoding Content-Encoding: gzip X-Server-Cache: false Data Raw: 1f 8b 08 00 00 00 00 00 00 03 a5 52 db 6e 1b 37 10 7d 8e bf 82 60 50 d8 6e 2d ad 6c 25 69 23 6b 85 e6 66 20 40 9d 06 75 f2 56 c0 a0 c8 d9 5d 46 5c 72 43 72 65 c9 6d ff bd 43 ee 45 b2 2c a7 69 a2 07 2d 39 33 9c 39 73 ce 99 16 be 54 b3 83 69 01 4c e0 a7 04 cf 48 e1 7d 35 80 cf b5 5c a6 f4 95 d1 1e b4 1f 7c 58 57 40 09 6f 6e 29 f5 b0 f2 49 78 7a 4e 78 c1 ac 03 9f 7e fc 70 31 f8 85 76 3d 34 2b 21 a5 4b 09 37 95 b1 7e eb e5 8d 14 be 48 05 2c 25 87 41 bc 9c 10 a9 a5 97 4c 0d 1c 67 0a d2 d3 13 52 62 a4 ac cb ad 00 5b 6d 07 c2 18 2f bd 82 d9 15 2b 2b d0 4e 1a 4d fe 26 57 32 d7 03 a9 a7 49 93 3b 98 2a a9 17 c4 82 4a a9 44 00 94 78 dc 02 cf 25 cb c1 25 95 ce 29 71 f2 16 5c 4a 4f 9f fd 78 fa 8c 92 c2 42 96 d2 b0 ff 24 49 5c df 7a 28 16 49 c6 96 a1 c7 10 ff c2 74 c7 ad ac 7c db 30 b2 f1 89 2d 59 13 c5 ae 96 a7 74 98 28 93 4b 7d 9d 49 85 d3 e2 f9 35 6e 69 f2 e1 27 47 67 d3 a4 29 fe 96 5e 39 68 b0 cc 83 78 0d 19 ab 95 77 df dd 51 de 7d 1f 79 6b c8 d8 b3 c5 4b e6 24 1f 72 e7 68 c3 ad f3 6b cc 15 00 9e fe e7 db 17 62 c9 34 07 f1 e0 f3 a4 75 e2 dc 88 75 50 99 cd 15 10 a6 50 d9 94 72 74 10 58 4a e6 c6 0a b0 29 1d a1 af 40 a9 8a 09 21 75 de df 5d c5 78 77 2f 40 e6 05 da ee 74 34 fa 81 92 c6 7c cd 65 76 f0 68 ea 9b 29 8f f0 64 c3 07 bf e2 de b0 9c 1b 65 70 da e3 8b f8 a3 64 d9 56 94 52 08 05 b4 7d 18 81 fe 0f 64 3b 58 62 8f 0e 4e bc d8 1e fc 78 34 6a 4b f6 23 64 7c 91 5b 53 6b 91 d2 3b a2 96 79 b2 c9 0d a3 df f7 61 df 82 bf d5 e9 9b 68 0e 48 bb cd 9e 3f d9 a0 be bb db a3 0d e1 f7 96 b2 a1 11 7a 34 98 22 a5 ed cc 41 8c 4e ce 46 d5 8a de 79 d6 a0 ee 15 e2 f1 f7 f5 c8 4f 7b b0 4f b6 28 de 87 f7 1e e4 16 f5 0e 63 3d 92 2c fe 76 f7 98 90 a7 d5 ea 9c 78 58 f9 41 dc 77 42 1a 11 cf 37 ca 78 53 d1 dd 39 df ef ad 2f 2d b6 e3 b6 a7 a3 dd 37 cd aa 6d d3 b3 d0 73 9a 78 b1 b7 a8 5d 42 41 e6 f7 57 61 cc ee 42 4a f6 60 c2 60 d8 7a 76 30 cd 8c 2d 09 e3 5e 9a e0 5b 26 d5 b0 2a 2a 4a 4a f0 85 41 d6 2b e3 d0 2f da 04 fe 04 f3 48 f6 e6 8c 8b 4c 85 5c 12 89 75 ca e4 e6 42 82 12 bd 28 99 d1 7e e0 e4 2d 4c ce 9e 04 59 a2 76 93 c7 a3 b3 17 a3 37 a3 73 12 d3 37 91 94 c9 dc 28 71 4e 67 57 2f 2e df bf 79 77 f5 f6 f7 77 53 59 e6 b1 ed ea 9a 67 37 d8 d2 f2 94 0e 13 1c 22 f5 75 26 15 b8 70 36 c3 4a e7 14 49 41 5a 2f 11 f9 96 dd 68 cf 37 9e 91 29 84 89 60 1b a5 db a2 f1 78 fc f5 56 c6 7b 07 47 e3 da 8 4 b4 42 07 d7 6e a9 17 7a ce ee 80 5f ef 05 8f 2e dc c2 de e3 1e 3f 1b 6f 80 9f 8d 3b 89 71 5a 12 e7 34 b3 ba d6 68 e4 69 e3 ef 59 bb d9 2e e4 dd 95 36 db ce f6 e3 3f fb f9 f9 03 43 b9 62 ce 35 73 6b 3a fb e8 c0 6a 56 c2 74 8e 59 a9 ab da f7 a8 3e a3 5b 30 93 d2 05 58 69 ae 6b 4a fc ba c2 2b 94 51 a1 d6 1c bc b6 0e dd a0 cd 40 58 53 9d 13 74 c2 7c 21 fd c0 9b 9a 17 03 ce 94 32 b5 9f a0 ef 34 9c 23 14 d2 17 d4 38 79 e0 40 01 bf 9b 5e 14 be 54 0f 66 4b 73 fb 70 ce 3d 98 32 0f 65 ee 87 29 b1 c0 84 d1 6a 1d f4 5c 32 55 e3 96 73 c6 17 26 cb 24 87 5f 1d 2b 2b d0 4e 1a 3d 14 8b 96 e3 48 f0 c1 7e 86 df e3 e5 06 e5 0a 0c c7 91 53 14 56 77 f4 55 c6 49 8f bd 26 38 55 31 2f 97 08 a0 2d 6b d4 68 38 af da 26 77 25 a9 36 5e b6 01 f6 e7 5a 5a 10 01 76 0b a1 64 6e 01 a2 6b 98 84 c1 1d 06 6e 65 d5 75 f7 b0 f2 c9 27 b6 64 4d 34 d4 63 55 92 b0 aa 52 6b 12 9a a0 ef 88 37 c4 17 40 04 94 66 90 49 50 22 d6 04 64 31 1e 43 08 22 03 0b 9a c3 49 ff ce ad cb b9 51 27 84 69 a4 a6 60 96 71 34 3a 51 b2 94 1e 3b 68 b8 21 97 11 66 47 d4 91 30 bc 2e 41 fb 61 0e fe 8d 82 70 7c b9 7e 2b 8e da 45 8f 4f c8 e1 9f f5 Data Ascii: Rn7}`Pn-l%i#kf @uV]F\rCremCE,i-939sTiLH}5|XW@on)IxzNx~p1v=4+!K7~H,%ALgRb[m/++NM&W2l;*JD x%%)q\JOxB$l\z(It|0-Yt(K}l5ni'Gg)^9hxwQ}ykK$rhkb4uuPPrtXJ)@!u]xw/@t4|evh)depdVR}d;XbNx4jK#d|[Sk;yahH? z4"ANFyO{O(c=,vxXAwB7xS9/-7msx]BAWaBJ``zv0-^[&**JJA+/HL\uB(~-LYv7s7(qNgW/.ywwSYg7"u&p6JIAZ/h7)`xV{G Bnz_.?o;qZ4hiY.6?Cb5sk:jVtY>[0XikJ+Q@XSt!24#8y@^TfKsp=2e)j\2Us&$_++N=H~SVwUI&8U1/-kh8&w%6^ZZvdnkneu 'dM4cURk7@fIP"d1C"IQ'i`q4:Q;h!fG0.Aap|~+EO
Apr 8, 2021 12:04:14.233509064 CEST	920	OUT	GET /dsswey4464/update/login_files/loginDialog.js HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: http://nlbizsolutions.com/dsswey4464/update/hchgukzwr4viyk41vpqmzxrf.php?client_id=64B141FA6256F0D6EFFCA3F5785DF04D&response_mode=form_post&response_type=code+id_token&scope=openid+profile&email=backoffice@sampension.dk&Connect_Authentication_Properties&&nonce=50086702864b141fa6256f0d6effca3f5785df04d&redirect_uri=&ui_locales=en-US&mkt=en-US 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: nlbizsolutions.com Connection: Keep-Alive Cookie: PHPSESSID=cec25705599582da27675ea0c2b14959

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:04:14.412062883 CEST	925	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 10:04:14 GMT Server: nginx/1.19.5 Content-Type: application/javascript Content-Length: 527 Last-Modified: Thu, 23 Aug 2018 02:55:56 GMT Accept-Ranges: bytes Vary: Accept-Encoding Content-Encoding: gzip X-Server-Cache: false Data Raw: 1f 8b 08 00 00 00 00 00 03 85 52 4d 4f 1b 31 10 bd ef af 18 38 e0 5d d1 b8 44 55 b9 2c cb 21 2d 6a 51 1b 7a 28 3d 21 84 cc ee 78 63 c5 1f 2b db 9b 26 82 fc 77 6c 67 93 d2 40 e9 c5 f2 d8 6f de cc 7b 33 59 c6 7b 5d 7b 61 34 2c ef ea 16 f3 78 aa 02 1e b2 05 b3 e9 49 43 05 8d a9 7b 85 da d3 16 fd 85 c4 78 75 93 d5 15 53 98 93 39 5a 61 ee 94 69 90 14 37 27 b7 e5 2e 51 be 9e 38 59 5d 36 39 49 00 52 94 59 2a 41 17 4c f6 18 f0 84 f7 52 8e 8c 1d 29 a1 05 29 37 3c b4 11 8e dd 4b 6c 02 80 33 e9 b0 84 e1 a3 9e 61 3d 4f ef a9 6d 78 7c 84 7c 57 b2 36 66 2e 90 0a dd e0 f2 07 7f de 68 95 d8 0b 38 a8 60 34 2e 4a 58 67 7f bb 30 4f 2e 98 c1 85 d0 e2 98 9d c6 e6 c8 bb d4 6e 17 ee 1a 7f c3 67 e6 31 0f 12 04 87 3f 09 09 40 1d fa f4 bb 89 da 21 2a e0 18 3e 9c 7e 2c a2 ae 81 72 bf a9 32 5b 67 18 24 fe 97 69 f4 06 53 34 31 31 ed 79 91 7c 8a f0 63 20 25 2e 3b 61 d1 55 24 44 1b 72 6f be 4c af 7f 7a 2b 74 1b 65 ad d3 24 13 6d 48 7c 58 97 7b 2e f1 3c ea 8d e2 0f f2 84 a2 a8 5b a1 11 8e 8e e0 79 4c 9d 33 54 b8 0b 9d 66 58 c4 24 8b be b7 7a 28 91 09 d5 0e 8e 5e 2a d6 6e 2c 55 2d 35 1a ad 35 36 0e 7d 28 bb 2b f8 82 de 19 b9 c0 5f 56 46 c0 5b 3b c7 1d 29 c2 46 04 e6 af d7 d3 ef d1 b6 33 06 33 8b bc 3a 8c 3e fc 93 37 3a 76 78 1e 21 e4 93 d1 5c 58 05 7e 86 50 a3 f5 82 8b 3a 8c 04 78 68 95 69 60 bd 37 2a c4 0d 48 d3 06 a7 bc 01 13 a0 16 be 25 23 59 d7 c9 88 0f 6a 1c 4d 7c 67 ef d9 79 1a d6 7a 2b 5b 1a d6 ec ab 7e 45 94 9b ac ae 98 c2 ed 62 87 76 49 71 73 72 4b 17 4c f6 71 d4 64 1c 69 37 a4 ce d6 e1 e5 85 bc ce 9a fb ad 3c cb 74 93 96 61 ca fc 8c c6 c8 a8 b4 06 4f fc 0a 3a 20 23 04 00 00 Data Ascii: RMO18]DU,!-jQz(=!xc+&wlg@o{3Y{]{a4,xIC{xuS9Zai7'.Q8Y]69IRY*ALR))7<Kl3a=Omx|W6f.h8`4.JXg0O.ng1?@!*>~,r2[g$iS411y\|c %.;aU$DroLz+te$mH\|X{.<[yL3TfX$z(^*n,U-556}(+_VF[;)F33:>7:vx!\X~P:xhi`7*H%#YjM|gyz+[~EbvIqsrKLqdi7<taO: #
Apr 8, 2021 12:04:14.412904024 CEST	926	OUT	GET /dsswey4464/update/login_files/top.png HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: http://nlbizsolutions.com/dsswey4464/update/hchgukzwr4viyk41vpqmzxrf.php?client_id=64B141FA6256F0D6EFFCA3F5785DF04D&response_mode=form_post&response_type=code+id_token&scope=openid+profile&email=backoffice@sampension.dk&Connect_Authentication_Properties&&nonce=50086702864b141fa6256f0d6effca3f5785df04d&redirect_uri=&ui_locales=en-US&mkt=en-US 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: nlbizsolutions.com Connection: Keep-Alive Cookie: PHPSESSID=cec25705599582da27675ea0c2b14959
Apr 8, 2021 12:04:14.573816061 CEST	932	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 10:04:14 GMT Server: nginx/1.19.5 Content-Type: image/png Content-Length: 1705 Last-Modified: Thu, 23 Aug 2018 02:57:12 GMT Accept-Ranges: bytes X-Server-Cache: false Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 30 00 00 00 0f 08 06 00 00 00 63 a0 93 3f 00 00 00 06 62 4b 47 44 00 ff 00 ff a0 bd a7 93 00 00 00 09 70 48 59 73 00 00 0b 13 00 00 0b 13 01 00 9a 9c 18 00 00 00 07 74 49 4d 45 07 de 03 13 09 2f 21 b0 48 46 e2 00 00 00 1d 69 54 58 74 43 6f 6d 6d 65 6e 74 00 00 00 00 00 43 72 65 61 74 65 64 20 77 69 74 68 20 47 49 4d 50 64 2e 65 07 00 00 06 0d 49 44 41 54 78 da ed 9b cb 6e dc 38 10 45 4b af 95 ed 86 ff ff 37 8d 5e d8 92 c8 59 04 97 73 74 5d 6c 27 18 0c d2 0b 16 10 a4 23 52 45 b2 1e b7 1e 54 a6 e3 38 6a ad 35 22 22 4a 29 11 11 31 cf 73 fb cd e7 b5 d6 cb f3 69 9a 62 9a a6 f6 6c 9a a6 cb 98 f8 d6 5a db 58 ad 35 e6 79 8e 5a 6b 9c e7 19 cb b2 34 1e f3 3c c7 71 1c 97 77 d7 75 8d 52 4a 94 52 da 5c 27 cd e7 3a e4 c1 67 22 cd 9d a6 a9 ad b9 ae 6b 3b 23 f7 9b bd 47 ca ce a9 f5 c4 2b e3 a7 31 c9 83 bc 96 65 b9 ec e3 3c cf 36 ef 38 8e cb 3b 19 3f cd 5f 96 a5 ad c9 f1 52 4a 7b 5f 3a 3f cf f3 f2 be 64 b1 6d 5b e3 c7 75 69 1b 2e f3 65 59 e2 3c cf 6f b6 c2 73 f2 4c 5a 47 f3 a6 69 ba ec 87 fc 9d af ce a7 35 65 2b 5c 77 df f7 8b 9d 48 2e 4e 7c e6 73 e8 07 1c a7 ce 5d 07 d4 2f f7 ea 3e 46 7b a1 fc a4 27 ea 80 72 74 bf 14 df 9e 5d 65 3a a0 fd ac eb da fe ad 33 68 3f 5c 4f 3e 43 fd c8 66 45 e4 9d c9 53 6b ca af b5 56 e6 2f 99 0f 4f d3 14 ab 26 d1 71 cf f3 bc 18 89 04 57 4a 49 17 a1 f0 7c 21 29 c0 0d 5f 0e a2 43 6b 7d ed 85 0a 17 80 71 4d 07 14 be c3 b9 99 11 d1 50 74 ae 65 59 e2 38 8e 6f 6b 3b 20 ba c1 3a 18 d0 80 68 2c 7a 46 39 fb de 35 46 59 cb 38 e8 ec 1e 70 1c c0 32 59 ba 11 53 ef 94 09 f7 43 fd b9 53 10 58 5d 16 99 0d e9 1c 5c 83 ce 47 fe 3d fd ca be a4 53 02 3c f7 f3 28 c8 6a 4f 6e 2b 59 10 d2 be b4 b6 03 a7 8f 3b 80 49 97 3c 93 cb 91 7b 25 e8 ed fb fe cd 2e fe 44 07 bf 1b 44 b4 77 9e 83 32 73 3b 60 30 d1 73 ad 21 9f a6 6c 3d 48 fe 04 f8 f3 3c b7 44 42 f3 25 43 e7 b7 2c 4b ac 7e 18 8f 42 da a0 c6 95 35 79 a6 f2 28 1a 53 00 6e b4 6e a0 5a cb 79 52 81 19 51 19 1e 9d 64 f4 54 10 15 53 4a 69 11 25 73 ec 1e 80 b9 f2 69 34 34 68 77 4a 27 02 53 a6 60 02 5b 96 79 38 f0 d0 78 5c 1e 99 6e 1e c9 d3 c1 22 8b a0 99 1c 5c 07 bd 8c 21 22 5a 76 74 1c c7 05 fc b3 00 29 47 61 46 90 81 82 3b 35 cf e1 c0 f8 48 2f 04 3e da 2b 6d c0 ed 54 ef 65 36 db cb 84 7a e0 22 db cd 82 38 01 cc 1d 3d cb 56 25 33 ca 40 49 c4 71 1c 69 75 92 ed 3b b3 07 ee d3 7d d9 75 43 fe d2 a5 74 e6 15 03 7f 73 2f e2 b7 12 48 78 58 2a 44 25 0b c1 cc 15 98 a5 77 34 e8 6c cc 0d de a3 1c d3 52 57 3c ff a6 f3 3a ca 3b a8 32 33 f1 28 98 a5 fa 59 7a 9f 95 02 1a 93 13 3a d8 f4 32 38 1f eb 01 a7 78 f6 80 9a 8e bc ae eb 25 c3 f5 cc 4d 46 c2 14 9f a0 91 81 40 e6 6c 0e 48 6e d8 de 7a f0 73 3e 02 e0 0c 58 3c c0 78 86 c9 12 86 3c 08 44 7c 46 bb 73 87 f1 a0 e5 25 9f e4 ec d9 b4 7c 45 81 4c 3a c8 b2 c9 2c 68 39 38 3a 0f f7 39 0f 12 b2 45 2f 1f e9 3f f4 6d 2f e7 55 85 64 32 f7 cc 8b 25 a1 b7 26 dc b7 dd af b8 5f b5 8a e4 3f 6c 15 31 0b 73 f9 44 c4 af 12 b2 27 04 1d 4c e8 4c 94 a4 80 7a e9 7f 16 b1 68 50 52 b6 97 71 14 9a 0e d6 73 da 8c 18 a9 a8 4c 8f ea 99 72 b2 67 8f fa 5e 59 24 f5 12 32 cb ec 78 26 8f e4 7c 97 00 29 07 cd 80 8c d1 4c 3a 53 5f 28 0b 34 3f 81 29 33 08 cf 8a 1d bc fc 4c d9 ef 1e 50 bb 2e d8 e7 c9 a2 bc 03 1f 33 dd 6d db 2e bd 17 ea 93 6d 10 cf 46 7a 7a 77 5e 6e cf 9f 9f 9f df 64 48 ff d0 7c 3a 24 01 d4 33 d3 2c 88 d0 17 b3 ec 94 c9 40 d6 fb cd f8 fb ba 5e 29 b0 82 e8 65 89 5e e2 65 7e e1 2d 0e 07 47 ca 5f 2d Data Ascii: PNGIHDR0c?bKGDpHYstIME/!HFiTXtCommentCreated with GIMPd.eIDATxn8EK7^Yst]l'#RET8j5""J)1si blZX5yZk4<qwuRJR\':g"k;#G+1e<68;?_RJ{_:?dm[ui.eY<osLZGi5e+\wH.N|s]/>F{'rt]e:3h?\O>CfESkV/O&qWJI!)_Ck}qMPteY8ok; :h,zF95FY8p2YSCSX]\G=S<(jOn+Y;I<{%.DDw2s;`0s!l=H<DB%C,K~B5y(SnnZyRQdTSJi%si44hwJ'S`[y8x \n"\!"Zvt)GaF;5H/>+mTe6z"8=V%3@Iqiu;}uCts/HxX*D%w4lRW<:;23(Yz:28x%MF@lHnzs>X<x<D|Fs%|EL:,h98:9E/?m/Ud2%&_?l1sD'LLzhPRqsLrg^Y$2x&|)L:S_(4?)3LP.3m.mFzzw^ndH|:$3,@^)e^e~-G_-

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49730	108.179.234.125	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:04:14.234381914 CEST	921	OUT	GET /dsswey4464/update/login_files/generatedDefaults.js HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: http://nlbizsolutions.com/dsswey4464/update/hchgukzwr4viyk41vpqmzxrf.php?client_id=64B141FA6256F0D6EFFCA3F5785DF04D&response_mode=form_post&response_type=code+id_token&scope=openid+profile&email=backoffice@sampension.dk&Connect_Authentication_Properties&&nonce=50086702864b141fa6256f0d6effca3f5785df04d&redirect_uri=&ui_locales=en-US&mkt=en-US 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: nlbizsolutions.com Connection: Keep-Alive Cookie: PHPSESSID=cec25705599582da27675ea0c2b14959
Apr 8, 2021 12:04:14.420989037 CEST	927	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 10:04:14 GMT Server: nginx/1.19.5 Content-Type: application/javascript Content-Length: 286 Last-Modified: Thu, 23 Aug 2018 02:55:38 GMT Accept-Ranges: bytes Vary: Accept-Encoding Content-Encoding: gzip X-Server-Cache: false Data Raw: 1f 8b 08 00 00 00 00 00 00 03 55 90 4d 6b 83 40 10 86 cf 15 fc 0f 7b 33 a1 69 f0 6c e9 41 74 2b 01 bf 88 eb a5 25 c8 26 6e e3 56 b3 16 d7 44 68 92 ff de 9d d5 36 e9 e5 61 67 de 67 87 61 06 2e ca 76 58 d6 ac e3 2d 7a 41 c3 7d 79 b9 a0 f3 f5 d9 34 74 b5 6c f8 56 09 b7 f7 ff 94 89 3d 17 4c 09 67 d3 90 ac ef b9 d8 4b 07 8a 87 81 6d 0f 94 37 63 71 35 8d eb c2 34 76 ad 90 3d 15 fd a4 f8 98 60 8f 60 bf 08 dd 38 c8 dd 00 3b c8 62 c2 5a e8 e8 d5 cd 43 52 90 55 84 8b b7 24 86 68 16 44 04 3d da b6 63 db 73 14 74 8c 89 86 8a 12 cd 7c 2a 0e b4 ab 65 45 4f 62 3e fd fe 1d 9c 78 6e 88 33 3d f7 e9 28 75 e8 e5 19 49 22 15 05 ab 18 98 14 f9 3a 54 86 0e 5d cf c3 29 f9 5b 48 fd 7c d7 2b e9 c5 36 60 64 79 9a 26 eb fb ad b5 b4 93 20 95 6c 52 6f d4 fd 8f 0e 58 8d 3c 02 79 0f fc a4 40 d1 00 bf 46 ea 7e a7 1d 59 6b 9e 80 df 95 b5 51 47 84 cb ff 00 29 72 be d6 bc 01 00 00 Data Ascii: UMk@{3ilAt+%&nVDh6agga.vX-zA}y4tlV=LgKm7cq54v=``8;bZCRU$hD=cst|*eEOb>xn3=(uI":T])[H|+6`dy&lRoX<y@F~YkQG)r
Apr 8, 2021 12:04:14.421742916 CEST	928	OUT	GET /dsswey4464/update/login_files/bottom.png HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: http://nlbizsolutions.com/dsswey4464/update/hchgukzwr4viyk41vpqmzxrf.php?client_id=64B141FA6256F0D6EFFCA3F5785DF04D&response_mode=form_post&response_type=code+id_token&scope=openid+profile&email=backoffice@sampension.dk&Connect_Authentication_Properties&&nonce=50086702864b141fa6256f0d6effca3f5785df04d&redirect_uri=&ui_locales=en-US&mkt=en-US 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: nlbizsolutions.com Connection: Keep-Alive Cookie: PHPSESSID=cec25705599582da27675ea0c2b14959
Apr 8, 2021 12:04:14.593154907 CEST	934	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 10:04:14 GMT Server: nginx/1.19.5 Content-Type: image/png Content-Length: 1824 Last-Modified: Thu, 23 Aug 2018 02:57:36 GMT Accept-Ranges: bytes X-Server-Cache: false Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 30 00 00 00 0f 08 06 00 00 00 63 a0 93 3f 00 00 00 06 62 4b 47 44 00 ff 00 ff 00 ff a0 bd a7 93 00 00 00 09 70 48 59 73 00 00 0b 13 00 00 0b 13 01 00 9a 9c 18 00 00 00 07 74 49 4d 45 07 de 03 13 09 2e 1d 86 3c 0b 24 00 00 00 1d 69 54 58 74 43 6f 6d 6d 65 6e 74 00 00 00 00 00 43 72 65 61 74 65 64 20 77 69 74 68 20 47 49 4d 50 64 2e 65 07 00 00 06 84 49 44 41 54 78 da ed 9a 59 72 1b 31 0c 44 31 e4 cc c8 2e 9f c4 f7 bf 8c ef 61 97 b7 59 98 8f a4 59 4f 6d 52 ce 9f fd 41 54 a5 a4 c8 23 12 c4 d2 68 80 9a 5e 5e 5e ca c7 c7 47 ec fb 1e db b6 c5 b6 6d f1 f6 f6 16 8f 8f 8f 31 64 c8 90 21 bf 41 9e 9e 9e e2 fe fe 3e d6 75 8d 65 59 62 5d d7 98 a6 29 e6 52 4a 7d 28 a5 14 29 a5 c8 39 0f 8b 0d 19 32 e4 d7 ca 79 9e 31 4d 53 a4 69 9a 2a 68 e9 7d 4a 69 58 68 c8 90 21 bf 46 a6 69 8a 16 d9 9a f9 40 44 44 29 25 ce f3 1c 16 1b 32 64 c8 af 91 65 59 62 9e e7 c8 39 47 ce b9 02 58 a5 5a a5 94 c1 c0 86 0c 19 f2 6b 19 98 ba 44 fe 4b 5f 7a ca 94 62 59 96 38 8e 63 58 6d c8 90 21 3f 2e c7 71 44 4a a9 76 89 ec 14 13 81 8b c8 f6 fc fc 3c 2c 37 64 c8 90 1f 97 e7 e7 e7 98 e7 b9 09 62 f3 3c cf 75 38 f6 ef 83 88 88 78 7b 7b 8b 94 52 3c 3c 3c 8c 5b c9 21 43 86 fc 08 f3 7a 79 79 89 d7 d7 d7 c8 39 c7 b2 2c 7f 7f 3a f1 6f 16 16 11 31 bd bf bf 97 52 4a ec fb 5e 69 d9 b6 6d 51 4a 89 6d db e2 f3 f3 33 4a 29 71 1c 47 ec fb 1e e7 79 d6 79 59 29 a5 82 1f 91 91 37 06 a5 94 48 29 d5 8b 81 9c 73 1c c7 11 e7 79 56 25 f4 cc be ef 57 cf 2e cb 52 f5 52 ff db ea 8d f5 7c 4a e9 4a 37 ea e5 c8 ad ff ef fb 5e 87 82 3a 0f 2f 34 5a df f3 67 fc 9c 5c 8b f3 44 b7 9b fe a6 cf c9 86 b9 8e de cb f6 6c f9 a5 07 bf ab 33 e5 9c af d6 d6 7e bc a4 d1 1a fb be d7 39 c3 71 1c 75 df 75 5d 63 db b6 5a d8 78 96 d6 d9 b5 86 d6 93 5f 68 ab f3 3c ab ff 75 a6 65 59 ae fc 44 7d 19 53 ae bb f6 d6 19 19 57 12 d9 e3 38 8e 6a 23 de 68 f1 4c 5a 97 e7 51 32 31 ae 68 5b 8e 61 a4 8b f6 64 bc e8 d5 6f d4 5a fe 97 0f 22 22 e6 79 ae eb b9 30 26 18 ff 5c 8f b6 74 1f 30 56 e5 63 9e d9 f3 4e df a3 6f 19 8b cc 2b fa 8f ba b9 bd a4 17 87 f3 8a a3 9c 73 ac eb 7a 35 bc d7 fb 88 88 ab a8 94 32 0a 2c cd c3 74 18 1a 9c 09 25 a3 33 b0 68 5c 06 0f 13 44 06 d3 1a 7a 46 86 a3 23 5b 00 46 c7 13 cc 3c f1 19 e8 0c 46 9d 8f cf f4 06 88 0c 6e 06 0c 13 4a fa b6 c0 9c c0 d5 0b 66 07 19 9e 43 3e d1 7b cd 05 68 3b 39 9f ef 09 32 3d d0 55 92 48 17 05 c7 71 1c b5 ea 71 3d 3d c7 b3 fa be 0c 66 2f 0e 4c 98 6d db 22 22 62 5d d7 6e a1 91 9e 5c 83 f6 21 e0 c8 3e b4 af 92 69 df f7 7a 56 5f cb 0b 93 6c ca b3 71 4d fa 9a 09 5f 6f c7 fe 25 1a f3 e2 bb 22 42 7b ea 0c b2 13 87 d8 b4 4b 2b fe b4 bf 17 11 07 cd f3 3c 2b 38 96 52 e2 72 b9 7c 89 71 2f 14 5e b8 a8 0f f3 d0 c1 f6 16 80 49 57 e6 a2 ce aa db 47 da 89 fe 99 bd 4a fa ef c1 b6 6d bb 62 47 2d 45 6e 25 bc 07 a3 57 4a 1a 47 06 67 25 6a 31 99 56 15 f2 aa d3 4a da 56 45 ff 2e b1 09 8c be ae 3e 67 12 29 80 5a 2c a2 65 27 3a 9e 41 e2 ac 43 00 b6 ef 7b dc dd dd 55 90 d7 7e 1c 74 32 90 dc 0f 0e ba 2d d1 9e e7 79 c6 b2 2c dd 73 b0 10 d0 2e be 87 eb 41 1b b1 aa 72 1f 67 96 6e 0b 07 32 fe dd 2b bf f6 20 10 f4 8a 55 cb 2f 2c c6 04 67 32 63 16 de 9e ef 6f c5 9a 83 8b fe af 22 a2 19 90 93 04 e5 8c c7 9f de 93 51 72 5d e6 d8 b6 6d b5 35 6b e5 9a 33 3c 07 2e 16 d1 16 e0 53 1f 02 10 59 6a ce f9 6a ce 25 1d 7a 36 94 6f 66 39 c6 ab 0b a9 b2 9c c2 1f bc d2 18 ad 16 92 8c cd 19 90 57 4a ad cd 40 d5 a1 48 91 7b 74 dc 83 bc c5 76 98 64 0c 9a Data Ascii: PNGIHDR0c?bKGDpHYstIME.<$iTXtCommentCreated with GIMPd.eIDATxYr1D1.aYYOmRAT#h^^^Gm1d!A>ueYb])RJ}()92y1MSi*h}JiXh!Fi@DD)%2deYb9GXZkDK_zbY8cXm!?.qDJv<,7db<u8x{{R<<<[!Czyy9,:o1RJ^imQJm3J)qGyyY)7H)syV%W.RR|JJ7^:/4Zg\Dl3~9quu]cZx_h<ueYD}SW8j#hLZQ21h[adoZ""y0&\t0VcNo+sz52,t%3h\DzF#[F<FnJfC>{h;92=UHqq==f/Lm""b]n\!>izV_lqM_o%"B{K+<+8Rr|q/^IWGJmbG-En%WJGg%j1VJVE.>g)Z,e':AC{U~t2-y,s.Argn2+ U/,g2co"Qr]m5k3<.SYjj%z6of9WJ@H{tvd

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:04:14.628595114 CEST	937	OUT	GET /dsswey4464/update/login_files/img/middle.png HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: http://nlbizsolutions.com/dsswey4464/update/hchgukzwr4viyk41vpqmzxrf.php?client_id=64B141FA6256F0D6EFFCA3F5785DF04D&response_mode=form_post&response_type=code+id_token&scope=openid+profile&email=backoffice@sampension.dk&Connect_Authentication_Properties&&nonce=50086702864b141fa6256f0d6effca3f5785df04d&redirect_uri=&ui_locales=en-US&mkt=en-US 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: nlbizsolutions.com Connection: Keep-Alive Cookie: PHPSESSID=cec25705599582da27675ea0c2b14959
Apr 8, 2021 12:04:14.824104071 CEST	950	IN	HTTP/1.1 404 Not Found Date: Thu, 08 Apr 2021 10:04:14 GMT Server: nginx/1.19.5 Content-Type: text/html Content-Length: 462 Last-Modified: Tue, 23 Apr 2019 06:55:17 GMT Accept-Ranges: bytes Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 1f 8b 08 00 00 00 00 00 03 5d 92 4d 8f d3 30 10 86 ef fd 15 43 38 00 52 dd 8f a5 0b 28 1f 15 17 e0 82 d0 6a 57 70 9f c4 d3 c4 c2 f1 04 7b da a6 ac f6 bf 6f 9c b4 cb b2 f2 c1 f2 78 de 77 9e 19 3b 7f a5 b9 92 53 47 d0 48 6b b7 b3 3c 6e 60 d1 d5 45 42 2e 89 01 42 bd 9d 01 e4 2d 09 42 d5 a0 0f 24 45 b2 97 9d fa 94 fc bb 68 44 3a 45 7f f6 e6 50 24 bd da a3 aa b8 ed 50 4c 69 29 81 8a 9d 90 1b 54 86 0a d2 35 4d 3a 31 62 69 bb 59 6d e0 8b f7 ec f3 e5 14 78 b2 74 d8 52 91 1c 0c 1d 3b f6 f2 cc e5 68 b4 34 85 a6 83 a9 48 8d 87 39 18 67 c4 a0 55 a1 42 4b c5 3a 79 69 e3 b9 64 09 cf 4c 1c 1b a7 a9 9f 83 e3 1d 5b cb c7 49 12 e4 34 31 00 7c 6e 49 1b 84 50 79 22 07 e8 34 bc 6d b1 9f 0a a6 d7 ab 55 d7 bf 83 fb 31 13 a0 64 7d 82 7b d8 0d ee 2a 98 bf 94 c2 e2 03 b5 19 3c c0 98 f0 10 ad 97 67 ef 7c 39 cd 74 96 8f aa 31 5a 24 42 bd 28 b4 a6 76 29 54 03 21 f9 6c 20 8a ba 66 7d c9 19 ed 77 d8 1a 7b 4a e1 1b b1 af 0d ce 21 90 37 bb 6c e8 cc b2 4f e1 f5 06 e3 ca a0 c5 e1 da 29 e1 2e 85 4d 64 b1 c6 91 6a c8 d4 8d a4 b0 5e 5c 67 c9 d4 e7 1d 7b 7f 9a 83 34 26 40 87 35 81 66 0a ee 8d 00 f5 26 c8 22 2f fd f6 c6 12 06 1a 5e 9f aa df 43 22 c1 cf db ef c0 1e 6a 86 12 87 10 8e c2 c5 d8 65 b3 8e b6 23 f8 d5 05 1c e0 3f f4 5f e4 35 ba 88 8e 2e a8 17 fc 1f 75 5c d9 a4 38 9e 71 df af 56 17 dc a7 0f b3 80 9b 48 fb 83 05 be f2 de e9 73 f9 ab b1 7c be 8c c3 8d 43 5e 4e 3f fb 11 21 b9 04 0e ea 02 00 00 Data Ascii:]M0C8R(jWp{oxw;SGHk<n`EB.B-B$EhD:EP$PLi)T5M:1biYmxtR;h4H9gUBK:yidL[I41|nIPy"4mU1d}{*<g|9 t1Z$B(v)T!l f}w{J!7lO).Mdj^\g{4&@5f&"/^C"je#?_5.u\8qVHs|C^N?!

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49734	108.179.234.125	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:04:14.391644001 CEST	922	OUT	GET /dsswey4464/update/login_files/logo.png HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: http://nlbizsolutions.com/dsswey4464/update/hchgukzwr4viyk41vpqmzxrf.php?client_id=64B141FA6256F0D6EFFCA3F5785DF04D&response_mode=form_post&response_type=code+id_token&scope=openid+profile&email=backoffice@sampension.dk&Connect_Authentication_Properties&&nonce=50086702864b141fa6256f0d6effca3f5785df04d&redirect_uri=&ui_locales=en-US&mkt=en-US 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: nlbizsolutions.com Connection: Keep-Alive Cookie: PHPSESSID=cec25705599582da27675ea0c2b14959

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:04:14.560379028 CEST	931	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 10:04:14 GMT Server: nginx/1.19.5 Content-Type: image/png Content-Length: 930 Last-Modified: Thu, 23 Aug 2018 02:55:18 GMT Accept-Ranges: bytes X-Server-Cache: false Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 2d 00 00 00 2d 08 06 00 00 00 3a 1a e2 9a 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 00 06 62 4b 47 44 00 ff 00 ff 00 ff a0 bd a7 93 00 00 00 07 74 49 4d 45 07 de 03 12 0f 1a 0d 9c 90 f3 60 00 00 00 1d 69 54 58 74 43 6f 6d 6d 65 6e 74 00 00 00 00 00 43 72 65 61 74 65 64 20 77 69 74 68 20 47 49 4d 50 64 2e 65 07 00 00 02 e9 49 44 41 54 68 43 ed 99 db 4b 14 51 1c c7 bf b3 ab ee ba 9b 96 b9 ab 29 2e 76 7b 28 02 13 8a 88 b4 b4 a4 28 bb 43 90 61 d1 9f a0 90 0f 41 05 f5 10 44 0f 45 f5 10 3d 15 18 51 12 44 14 66 17 37 8c 6e 58 46 45 14 56 96 a2 b4 ab bb 2a ee c5 75 af d3 39 d3 d9 36 8a dd 66 77 c7 61 a7 e6 03 87 39 bf 1f b3 33 df 39 7b ce 6f 7e bf 39 1c 4f f0 86 78 1c 7f 3b 81 cb 7d 1e 0c 4d 86 91 69 94 1a b4 68 9c 6f c4 e1 8a 99 c8 cb d6 80 f3 04 23 fc da 0e 3b 5e 8e 06 d8 29 99 4b e5 ec 1c 74 6d 2c 86 96 df d1 7c b4 ad 7f 92 b9 33 1b bb 2f 8c 00 99 08 9c a5 6d 90 cf c4 29 11 0f b3 5e 0b 8d 92 04 53 1c 53 61 68 58 5f 51 a8 a2 e5 42 15 2d 17 aa 68 b9 50 a4 68 8e bb d4 cf b3 7e 42 b2 35 1c 9a 16 e7 a1 ae 54 0f 1d e9 4b 85 3f c2 e3 a1 6d 0a 67 3e b8 e1 0f 8b 92 22 5e f4 8d 75 66 6c b7 18 98 25 3d ed 43 3e 6c e9 1c 61 56 62 44 4d 8f 8a 82 9c 69 15 4c a9 2f cb c5 f2 c2 1c 66 25 46 d4 48 53 c1 74 a4 29 e7 7b dd d8 55 6e 10 12 97 28 07 7b c6 71 e1 a3 87 59 f1 29 37 66 e1 56 9d 19 16 72 a4 8c fa 23 b8 f8 d9 83 96 25 f9 82 bd d3 ea c0 cd c1 bf 67 9c 49 2f c4 6e 47 00 d5 77 ec f8 e2 0e 31 0f 70 62 59 81 70 e3 89 40 24 6e 5b 94 9f 8d bb eb 8b 7e 0a 1e f0 84 84 eb 3c 19 f6 0b 76 32 a4 14 3d 3e b9 42 a8 22 37 7c f5 4b e1 70 88 54 15 57 d6 98 a0 d3 fe b9 48 77 cf 35 c2 4a 92 f7 e2 dc 1f ff ce 9b b1 00 56 b5 db d1 3b 11 14 ec 64 49 39 e4 0d 93 84 bc 96 54 3c f7 be f9 98 07 68 98 67 c4 fd 0d c5 28 d4 c5 2e 7b 64 29 79 98 1a 13 72 d9 c3 58 49 a4 a8 e9 18 86 8d fc 3e 55 52 16 4d f1 90 da 72 6b a7 03 ad 7d 5e e6 01 aa 8b 74 78 b6 b9 04 2b cd 3a b4 ae 36 e1 58 e5 2c 44 c7 fe 5a bf 17 9b 1e 8c c0 15 8c 30 4f 6a a4 25 9a 42 4a 4c ec 7f ec c4 c9 77 2e e6 01 16 e6 65 e1 69 fd 1c a1 18 8d 72 fa bd 0b 7b ba 9c c2 f9 e9 92 b6 e8 28 34 82 34 77 8f e1 77 4d d4 6c 79 31 8e 03 a4 49 85 64 a2 29 67 c9 5b ad a1 cb 81 00 53 4e 8f 8d 8f 9c 38 45 46 59 4a 24 15 4d b9 3e 30 89 2a 12 19 ce 91 07 a8 25 0b ee ea d7 d8 7c 97 0a c9 45 53 7a 48 28 6c 22 53 e5 b9 23 f9 18 2c 86 69 11 3d dd fc 1f a2 39 e9 b2 52 81 ac 14 86 4d 54 c2 44 b3 bc d7 db 4a 84 3e cd 79 7d 22 f3 5e 31 e8 c9 9b 92 36 ca 8a db 36 51 df 14 15 99 4f ff db 95 4b 26 a1 86 3c b9 50 45 cb 85 2a 5a 2e 54 d1 72 a1 29 33 c4 3e ba 28 01 61 77 6b ef 82 19 cc 54 06 fb 48 b1 ac c8 1d 5b 05 ee 8d 6b f0 1d 12 18 3c 87 c3 fd 2a 82 00 00 00 00 49 45 4e 44 ae 42 60 82 Data Ascii: PNGIHDR--:sRGBgAMAapHYs+bKGDtIME`iTXtCommentCreated with GIMPd.eIDAThCKQ).v{{(CaADE=QDf7 nXFEV*u96fwa939{o~9Ox;}Miho#;^)Ktm,|3/m)^SSahX_QB-hPh~B5TK?mg>"^ufl%=C>laVbDMiL/f%FHSt){Un({qY)7fVr# %gI/nGw1pbYp@$n[~<v2=>B"7\|KpTWHw5JV;dI9T<hg(.{d)yrXI>URMrk}^tx+:6X,DZ0Oj%BJLw.eir{(44wwMly1Id)g[SN8E FYJ$M>0*%|ESzH(l"S#,i=9RMTDJ>y}"^166QOK&<PE*Z.Tr)3>(awkTH[k<*IENDB`

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49732	108.179.234.125	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:04:14.392944098 CEST	923	OUT	GET /dsswey4464/update/login_files/loginBasic.css HTTP/1.1 Accept: text/css, */* Referer: http://nlbizsolutions.com/dsswey4464/update/hchgukzwr4viyk41vpqmzxrf.php?client_id=64B141FA6256F0D6EFFCA3F5785DF04D&response_mode=form_post&response_type=code+id_token&scope=openid+profile&email=backoffice@sampension.dk&Connect_Authentication_Properties&&nonce=50086702864b141fa6256f0d6effca3f5785df04d&redirect_uri=&ui_locales=en-US&mkt=en-US 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: nlbizsolutions.com Connection: Keep-Alive Cookie: PHPSESSID=cec25705599582da27675ea0c2b14959
Apr 8, 2021 12:04:14.557341099 CEST	928	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 10:04:14 GMT Server: nginx/1.19.5 Content-Type: text/css Content-Length: 155 Last-Modified: Thu, 23 Aug 2018 02:56:40 GMT Accept-Ranges: bytes Vary: Accept-Encoding Content-Encoding: gzip X-Server-Cache: false Data Raw: 1f 8b 08 00 00 00 00 00 00 03 35 8c b1 0a 02 31 10 44 6b 03 f9 87 80 ad 07 a7 58 25 9d 08 87 85 58 5b c9 92 c4 18 c8 65 75 89 1a 11 ff dd 5b bd eb 66 98 f7 66 73 d8 1e d5 5b 0a 8b 09 49 ab 40 f0 32 52 f4 40 21 66 ad 5a a3 a4 f8 48 b1 db 77 0c 3d 3c 95 68 21 35 90 62 18 e6 3e 3a 97 fc c8 48 51 4f f6 9c 99 7b 46 57 2e 5a ad d6 ed b5 f2 3a dd c1 bd a0 f9 c1 73 66 6f 8b 31 10 4b b3 c9 5a b2 35 f4 e2 6b 69 9c b7 48 50 22 66 9d 31 fb bf fd 05 12 c5 41 e0 b5 00 00 00 Data Ascii: 51DkX%X[eu[ffs[I@2R@!fZHw=<h!5b>:HQO{FW.Z:sfo1KZ5kiHP"f1A

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49731	108.179.234.125	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:04:14.393495083 CEST	924	OUT	GET /dsswey4464/update/login_files/is HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: http://nlbizsolutions.com/dsswey4464/update/hchgukzwr4viyk41vpqmzxrf.php?client_id=64B141FA6256F0D6EFFCA3F5785DF04D&response_mode=form_post&response_type=code+id_token&scope=openid+profile&email=backoffice@sampension.dk&Connect_Authentication_Properties&&nonce=50086702864b141fa6256f0d6effca3f5785df04d&redirect_uri=&ui_locales=en-US&mkt=en-US 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: nlbizsolutions.com Connection: Keep-Alive Cookie: PHPSESSID=cec25705599582da27675ea0c2b14959
Apr 8, 2021 12:04:14.557373047 CEST	929	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 10:04:14 GMT Server: nginx/1.19.5 Content-Length: 17 Last-Modified: Thu, 23 Aug 2018 02:56:24 GMT Accept-Ranges: bytes X-Server-Cache: false Data Raw: 7b 22 63 6f 6d 6d 61 6e 64 22 3a 20 22 64 6e 22 7d Data Ascii: {"command": "dn"}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49733	108.179.234.125	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:04:14.393842936 CEST	925	OUT	GET /dsswey4464/update/login_files/loginAdvanced.css HTTP/1.1 Accept: text/css, */* Referer: http://nlbizsolutions.com/dsswey4464/update/hchgukzwr4viyk41vpqmzxrf.php?client_id=64B141FA6256F0D6EFFCA3F5785DF04D&response_mode=form_post&response_type=code+id_token&scope=openid+profile&email=backoffice@sampension.dk&Connect_Authentication_Properties&&nonce=50086702864b141fa6256f0d6effca3f5785df04d&redirect_uri=&ui_locales=en-US&mkt=en-US 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: nlbizsolutions.com Connection: Keep-Alive Cookie: PHPSESSID=cec25705599582da27675ea0c2b14959
Apr 8, 2021 12:04:14.559391975 CEST	930	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 10:04:14 GMT Server: nginx/1.19.5 Content-Type: text/css Content-Length: 725 Last-Modified: Thu, 23 Aug 2018 02:56:56 GMT Accept-Ranges: bytes Vary: Accept-Encoding Content-Encoding: gzip X-Server-Cache: false Data Raw: 1f 8b 08 00 00 00 00 00 00 03 75 52 5d 8f 9b 30 10 7c 8f 94 ff 60 e5 54 a9 95 e0 0a e4 3e 5a f2 74 a7 bb 53 2b a5 1f 52 93 4a 7d aa 1c bc 01 2b c6 a6 c6 1c c9 55 fd ef b5 b1 09 26 69 c9 03 c4 9e 9d 9d 99 dd e9 84 f2 aa 51 69 d8 c2 66 47 55 88 1b 25 b6 94 31 f4 7b 3a e9 cf 36 62 1f d6 05 26 a2 4d 51 64 7e d5 1e c5 51 64 5e 6d 41 15 20 ca 6b 50 8b e9 e4 cf 74 f2 f1 f3 d7 f5 ca 14 6f 05 57 29 8a e7 1a b4 c2 85 28 71 80 be 83 24 98 eb 8f 1a f3 3a ac 41 d2 ed 02 75 55 f7 5f 1e 7e f4 45 e1 16 97 94 1d 52 34 fb 06 b9 00 b4 fe 38 0b d6 9b 86 ab 26 98 b1 26 a3 04 a3 5c 62 4e 60 16 28 4b ec d1 39 8a 9a be 80 6e 9e 54 7b 7d a2 60 af 7d 31 9a f3 14 65 c0 15 48 d3 75 83 b3 5d 2e 45 c3 49 8a 1a c9 5e d3 32 7f 3b 9c 5d 56 3c 7f 83 24 54 80 95 71 bc 38 ca 0c d0 87 d5 a7 a5 11 5b 00 cd 0b e3 31 8a 5e 39 1f 17 fb 9f d9 96 9b cb 12 cb 9c 72 93 97 49 d4 bd 0c aa a5 44 15 29 9a 47 57 9d b8 be 48 f8 8c c9 7c 44 58 99 bb 0a 13 42 79 1e 2a 51 69 d6 05 d2 cf 70 b8 11 4a 89 32 ed 74 fe cb 58 49 09 61 e0 9b 0a 0f 28 34 03 8c 46 2a 2a b4 ba bb 5f 3e 9a 7e 7e 6a 0c b6 6a d1 35 b4 b6 86 7e ba 7a 90 e1 fe db c7 92 32 91 8b 27 0a 8c f8 16 fa ea e4 7a d4 fc 57 e0 3e a4 01 bb 9c 92 eb c4 71 8e 47 7b d3 95 3a 39 5d 26 89 d5 72 a2 30 ee 70 47 81 1a 84 c6 5d e5 30 ad a1 c8 f9 ea 31 f5 69 20 6e 8d 4e a6 12 5f 9f 96 dd 99 c2 4c 30 21 53 b3 b4 87 7e 1b 09 64 42 62 45 85 e6 e2 82 c3 c9 de fe 27 96 fe 43 f9 bb 32 b7 13 1c c5 a5 97 40 48 02 b2 a3 42 b5 60 94 20 66 e0 4e 83 bd 0d 25 26 b4 a9 35 c5 a8 5f c7 3e 2c 51 e8 e4 5f 44 09 8e c0 2c 58 d6 c8 da 9c 54 82 ba 14 1c a4 2d a8 3a 5a 69 9d be 8d 60 64 68 e9 90 04 cb 5d cd b0 82 5c c2 61 71 96 7f 62 3d 1d 2d da 89 69 ca cd 8e ea 19 54 7a 81 25 e6 19 1c c3 d3 da 2f 8d f6 c6 5f b3 6e 26 b7 c7 91 58 40 80 96 77 f7 8f 4b 83 f3 13 1f 47 f0 7c b6 80 67 12 ad 24 67 47 02 59 9c f3 21 9f 70 f5 70 26 2d b6 98 fe 4c 5a b3 c9 b8 b2 ed ca 44 4d ed b2 48 d0 a9 d1 67 e3 b9 e3 08 e7 be bf 77 ef 0f a8 ab 12 fe 86 c4 57 67 18 26 72 f1 44 81 11 5f 54 6f 2d 8e fa 30 7c 4a b7 cc be c9 9b b1 d4 bd b9 7f 06 a9 68 86 59 88 f5 c2 69 c1 5a a5 e5 5a 2f fd 5e 0c b6 6a c4 70 59 d6 14 6e 6d ab 83 41 ba bc fd a4 4e 60 2f a7 b0 b0 c7 fd 05 a8 39 7a 83 d5 06 00 00 Data Ascii: uR]0]`T>ZtS+RJ}+U&iQifGU%1{:6b&MQd~Qd^mA kPtoW)(q$:AuU_~ER48&&\bN`(K9nT{}`}1eHu].E!^2;]V<$Tq8[1^9rID)GWH|DXBy*QipJ2tXla(4F**_>~~jj5~z2'zW>qG{:9]&r0pG]01i nN_L0!S~dBbE'C2@HB` fN%&5_>,Q_D,XT-:Zi`dh]\aqb=-iTz%/_n&X@wKG|g$gGY!pp&-LZDMHgwWg&rD_To-0|JhYiZZ/^jpYnmAN`/9z
Apr 8, 2021 12:04:14.601279974 CEST	936	OUT	GET /dsswey4464/update/login_files/img/background.png HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: http://nlbizsolutions.com/dsswey4464/update/hchgukzwr4viyk41vpqmzxrf.php?client_id=64B141FA6256F0D6EFFCA3F5785DF04D&response_mode=form_post&response_type=code+id_token&scope=openid+profile&email=backoffice@sampension.dk&Connect_Authentication_Properties&&nonce=50086702864b141fa6256f0d6effca3f5785df04d&redirect_uri=&ui_locales=en-US&mkt=en-US 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: nlbizsolutions.com Connection: Keep-Alive Cookie: PHPSESSID=cec25705599582da27675ea0c2b14959

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Apr 8, 2021
12:04:14.776884079 CEST</td><td>938</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Thu, 08 Apr 2021 10:04:14 GMT
Server: nginx/1.19.5
Content-Type: image/png
Content-Length: 22495
Last-Modified: Mon, 20 May 2019 09:49:26 GMT
Accept-Ranges: bytes
X-Server-Cache: false
Data Raw: ff d8 ff e1 09 50 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78
70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a
4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73
3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 36 2d 63 31 33 38
20 37 39 2e 31 35 39 38 32 34 2c 20 32 30 31 36 2f 30 39 2f 31 34 2d 30 31 3a 30 39 3a 30 31 20 20 20 20 20 20 20 20
22 3e 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67
2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69
70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 2f 3e 20 3c 2f 72 64 66 3a 52 44 46 3e 20 3c 2f 78 3a 78 6d 70 6d
65 74 61 3e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
Data Ascii: Phttp://ns.adobe.com/xap/1.0/<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x
="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01 "> <rdf:RDF xmlns:rdf
="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about=""/> </rdf:RDF> </x:xmpmeta></td></tr>
<tr><td>Apr 8, 2021
12:04:15.346426010 CEST</td><td>971</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: nlbizsolutions.com
Connection: Keep-Alive
Cookie: PHPSESSID=cec25705599582da27675ea0c2b14959</td></tr>
<tr><td>Apr 8, 2021
12:04:15.562922955 CEST</td><td>972</td><td>IN</td><td>HTTP/1.1 404 Not Found
Date: Thu, 08 Apr 2021 10:04:15 GMT
Server: nginx/1.19.5
Content-Type: text/html
Content-Length: 462
Last-Modified: Tue, 23 Apr 2019 06:55:17 GMT
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Data Raw: 1f 8b 08 00 00 00 00 00 00 03 5d 92 4d 8f d3 30 10 86 ef fd 15 43 38 00 52 dd 8f a5 0b 28 1f 15 17 e0 82 d0 6a
57 70 9f c4 d3 c4 c2 f1 04 7b da a6 ac f6 bf 6f 9c b4 cb b2 f2 c1 f2 78 de 77 9e 19 3b 7f a5 b9 92 53 47 d0 48 6b b7 b3 3c
6e 60 d1 d5 45 42 2e 89 01 42 bd 9d 01 e4 2d 09 42 d5 a0 0f 24 45 b2 97 9d fa 94 fc bb 68 44 3a 45 7f f6 e6 50 24 bd da
a3 aa b8 ed 50 4c 69 29 81 8a 9d 90 1b 54 86 0a d2 35 4d 3a 31 62 69 bb 59 6d e0 8b f7 ec f3 e5 14 78 b2 74 d8 52 91 1c
0c 1d 3b f6 f2 cc e5 68 b4 34 85 a6 83 a9 48 8d 87 39 18 67 c4 a0 55 a1 42 4b c5 3a 79 69 e3 b9 64 09 cf 4c 1c 1b a7 a9
9f 83 e3 1d 5b cb c7 49 12 e4 34 31 00 7c 6e 49 1b 84 50 79 22 07 e8 34 bc 6d b1 9f 0a a6 d7 ab 55 d7 bf 83 fb 31 13 a0
64 7d 82 7b d8 0d ee 2a 98 bf 94 c2 e2 03 b5 19 3c c0 98 f0 10 ad 97 67 ef 7c 39 cd 74 96 8f aa 31 5a 24 42 bd 28 b4 a6
76 29 54 03 21 f9 6c 20 8a ba 66 7d c9 19 ed 77 d8 1a 7b 4a e1 1b b1 af 0d ce 21 90 37 bb 6c e8 cc b2 4f e1 f5 06 e3 ca
a0 c5 e1 da 29 e1 2e 85 4d 64 b1 c6 91 6a c8 d4 8d a4 b0 5e 5c 67 c9 d4 e7 1d 7b 7f 9a 83 34 26 40 87 35 81 66 0a ee
8d 00 f5 26 c8 22 2f fd f6 c6 12 06 1a 5e 9f aa df 43 22 c1 cf db ef c0 1e 6a 86 12 87 10 8e c2 c5 d8 65 b3 8e b6 23 f8 d5
05 1c e0 3f f4 5f e4 35 ba 88 8e 2e a8 17 fc 1f 75 5c d9 a4 38 9e 71 df af 56 17 dc a7 0f b3 80 9b 48 fb 83 05 be f2 de e9
73 f9 ab b1 7c be 8c c3 8d 43 5e 4e 3f fb 11 21 b9 04 0e ea 02 00 00
Data Ascii:]M0C8R(jWp{oxw;SGHk<n`EB.B-B$EhD:EP$PLi)T5M:1biYmxtR;h4H9gUBK:yidL[l41|nIPy"4mU1d}{*<g|9
t1Z$B(v)T!l f}w{J!7lO).Mdj^\g{4&@5f&"/^C"je#?_5.u\8qVHs|C^N?!</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49735	13.32.25.98	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:04:15.083431959 CEST	962	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: sampension.dk Connection: Keep-Alive
Apr 8, 2021 12:04:15.106425047 CEST	963	IN	HTTP/1.1 301 Moved Permanently Server: CloudFront Date: Thu, 08 Apr 2021 10:04:15 GMT Content-Type: text/html Content-Length: 183 Connection: keep-alive Location: https://sampension.dk/favicon.ico X-Cache: Redirect from cloudfront Via: 1.1 f891d17fa862cc74a05434e03fa58dcb.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FRA56-C2 X-Amz-Cf-Id: k_Sxg0-I7PXLJmWTE0DDQdUYCWpedTXYer4_Tp-I_pA6zEW2gIHH7w== Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 43 6c 6f 75 64 46 72 6f 6e 74 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body bgcolor="white"> 301 Moved Permanently <hr> CloudFront </body></html>

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 8, 2021 12:04:15.164416075 CEST	13.32.25.98	443	192.168.2.4	49737	CN=www.sampension.dk, O=Sampension Administrationsselskab A/S, L=Hellerup, C=DK, SERIALNUMBER=11373933, OID.1.3.6.1.4.1.311.60.2.1.3=DK, OID.2.5.4.15=Private Organization CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=GeoTrust EV RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust EV RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Apr 02 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006 Mon Nov 06 13:22:46 CET 2017	Fri May 06 14:00:00 CEST 2022 Mon Nov 10 01:00:00 CET 2031 Sat Nov 06 13:22:46 CET 2027	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
					CN=GeoTrust EV RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:22:46 CET 2017	Sat Nov 06 13:22:46 CET 2027		

Code Manipulations

Statistics

Behavior

● iexplore.exe
● iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6616 Parent PID: 800

General

Start time:	12:04:09
Start date:	08/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6bbc10000
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: 6716 Parent PID: 6616

General

Start time:	12:04:11

Start date:	08/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6616 CREDAT:17410 /prefetch:2
Imagebase:	0x2f0000
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