ID: 433392
Cookbook: browseurl.jbs
Time: 18:07:24
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

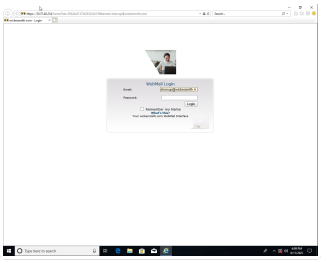
Analysis Report http://blockstyerts.live/sharcup@wicke…

Overview

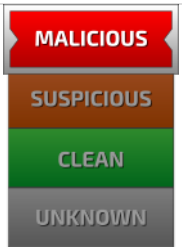
General Information

Sample URL:	http://blockstyerts.live/sharcup@wickersmith.com
Analysis ID:	433392
Infos:	

Most interesting Screenshot:



Detection



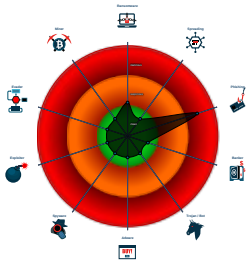
HTMLPhisher

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

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected HtmlPhish10
- Yara detected Phisher
- HTML body contains low number of …
- HTML title does not match URL
- URL contains potential PII (phishing…

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 5556 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4420 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5556 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\sharcup@wickersmith[1].htm	JoeSecurity_Phisher_2	Yara detected Phisher	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\home[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

Phishing:

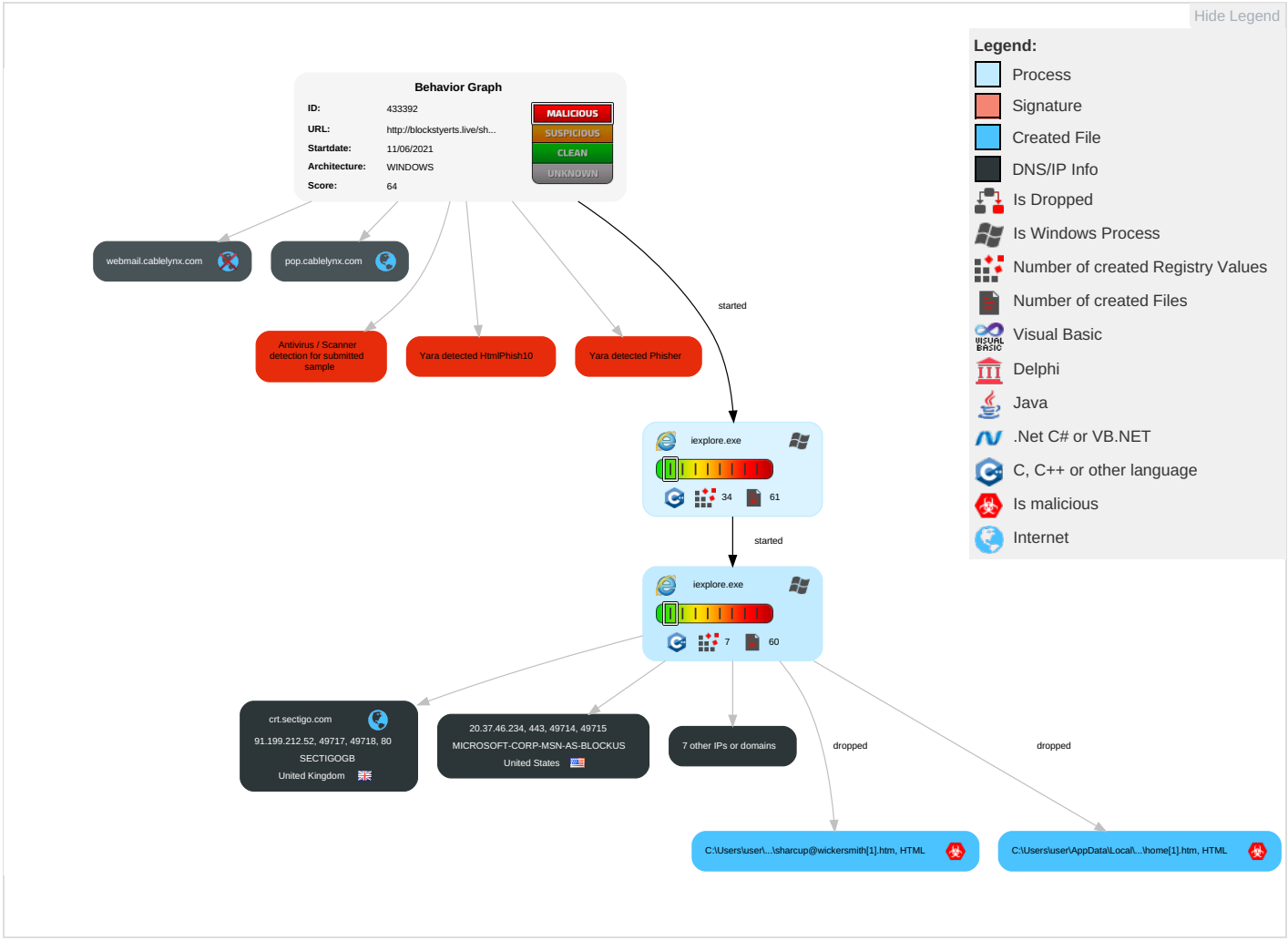
Yara detected HtmlPhish10

Yara detected Phisher

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 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 3	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 1	SIM Card Swap		Carri Billin Fraud

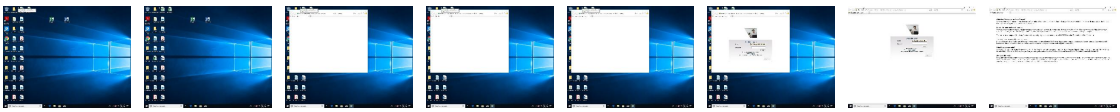
Behavior Graph

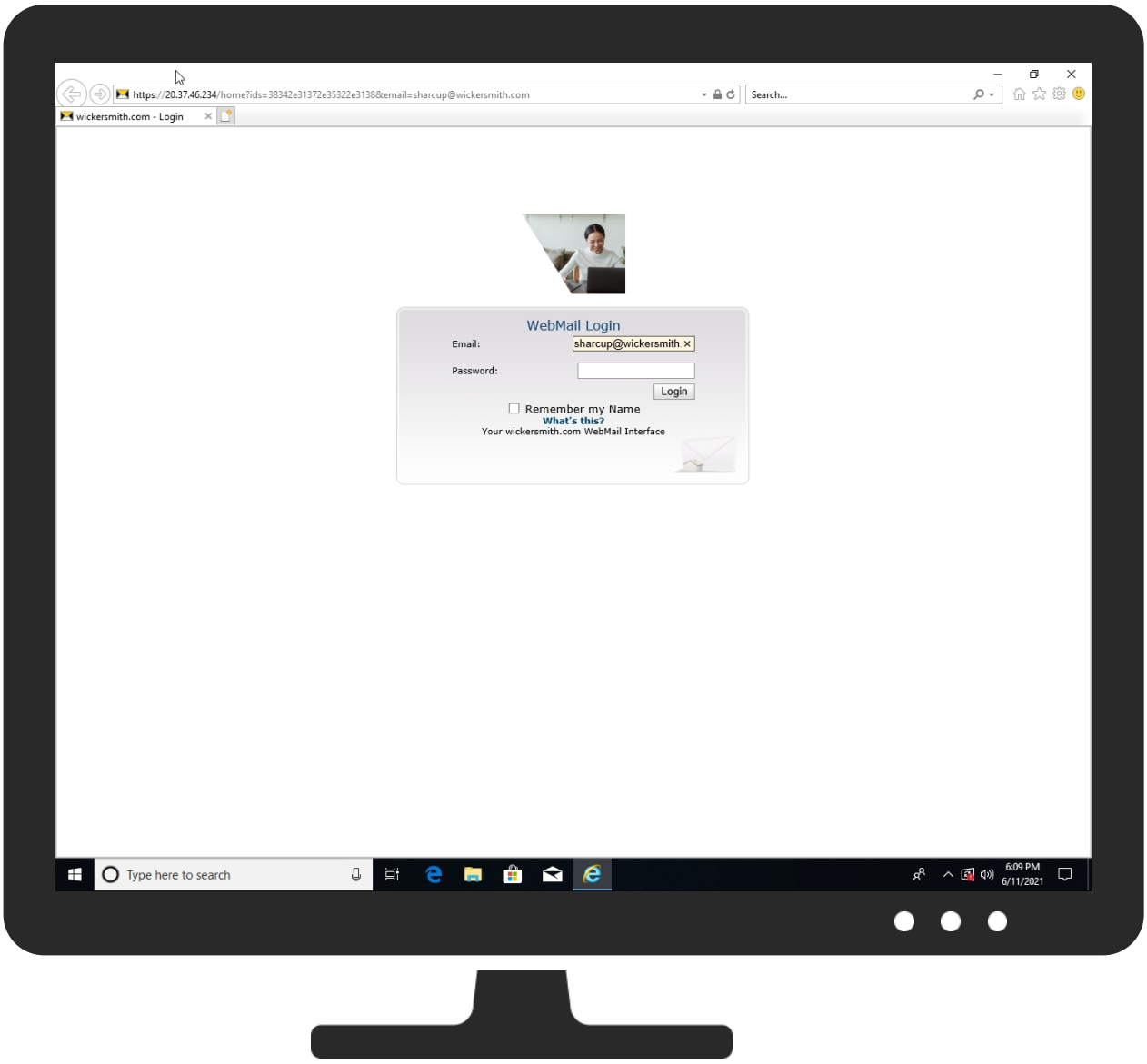


Screenshots

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://blockstyerts.live/sharcup@wickersmith.com	0%	Virustotal		Browse
http://blockstyerts.live/sharcup@wickersmith.com	0%	Avira URL Cloud	safe	
http://blockstyerts.live/sharcup@wickersmith.com	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
blockstyerts.live	0%	Virustotal		Browse
crt.sectigo.com	1%	Virustotal		Browse
zerossl.crt.sectigo.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://20.37.46.234/hve/sharcup	0%	Avira URL Cloud	safe	
http://https://20.37.46.Root	0%	Avira URL Cloud	safe	
http://zerossl.crt.sectigo.com/ZeroSSLRSADomainSecureSiteCA.crt	0%	Avira URL Cloud	safe	
http://www.wizard.ca	0%	Avira URL Cloud	safe	
http://www.lalit.org/lab/javascript-css-font-detect/	0%	Avira URL Cloud	safe	
http://https://20.37.46.8b73e0fa294bf6684fa38d	0%	Avira URL Cloud	safe	
http://https://20.37.46.ynx.com/webmail/plugins/login_auto/security.en.phpmith.comRoot	0%	Avira URL Cloud	safe	
http://https://webmail.cablelome?ids=38342e31372e35322e3138&email=sharcup	0%	Avira URL Cloud	safe	
http://www.stucox.com/blog/you-cant-detect-a-touchscreen/	0%	Avira URL Cloud	safe	
http://magicmail.linuxmagic.com/	0%	Avira URL Cloud	safe	
http://www.linuxmagic.com/	0%	Avira URL Cloud	safe	
http://https://webmail.cablel	0%	Avira URL Cloud	safe	
http://blockstyerts.live/sharcup	0%	Avira URL Cloud	safe	
http://https://20.37.46.234/?sharcup	0%	Avira URL Cloud	safe	
http://https://20.37.46.234/home?ids=38342e31372e35322e3138&email=sharcup	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
d26p066pn2w0s0.cloudfront.net	13.32.25.43	true	false		high
blockstyerts.live	52.161.162.59	true	false	• 0%, Virustotal, Browse	unknown
crt.sectigo.com	91.199.212.52	true	false	• 1%, Virustotal, Browse	unknown
pop.cablelynx.com	69.60.184.109	true	false		high
webmail.cablelynx.com	unknown	unknown	false		high
zerossl.crt.sectigo.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
logo.clearbit.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://zerossl.crt.sectigo.com/ZeroSSLRSADomainSecureSiteCA.crt	false	• Avira URL Cloud: safe	unknown
http://https://20.37.46.234/home?ids=38342e31372e35322e3138&email=sharcup@wickersmith.com	true		unknown
http://https://webmail.cablelynx.com/webmail/plugins/login_auto/security.en.php	false		high
http://blockstyerts.live/sharcup@wickersmith.com	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
20.37.46.234	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
91.199.212.52	crt.sectigo.com	United Kingdom		48447	SECTIGOGB	false
69.60.184.109	pop.cablelynx.com	United States		4452	AMERICAUS	false
52.161.162.59	blockstyerts.live	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
13.32.25.43	d26p066pn2w0s0.cloudfront.net	United States		7018	ATT-INTERNET4US	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433392
Start date:	11.06.2021
Start time:	18:07:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://blockstyerts.live/sharcup@wickersmith.com
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	10
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@3/26@5/6
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://webmail.cablelynx.com/webmail/plugins/login_auto/security.en.php
Warnings:	Show All

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\LocalLow\Microsoft\CryptnetUrlCache\Content\10BDC45B4A27319429BBC4F08A4E8A10	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	3506
Entropy (8bit):	7.54155945514523
Encrypted:	false
SSDEEP:	48:m4qXYiteL8B0wtUJgVXpxi4sVQmjPOZphFRl1P4qXYiteL8B0wtUJgVXpxi4sVQO:StO+0mrZn/T5RptO+0mrZn/T5R+
MD5:	5C8E451E4A7E09535AB02C6301187E84
SHA1:	CE337AB88CDAD351169A54668C6651E37D2C3A58
SHA-256:	3BEE4411F74C082D025884DA0688FE633DF567E220D9D17FD2733AF378123E5C
SHA-512:	2B7948258DB6C51A266E356B89B7659866220FE916CC051E0C26563E9D729500A73163DA21686FBAB15F9AED9CB240F3658F6F69DF8863FDDE6E8CA81940DA14
Malicious:	false
Reputation:	low
Preview:	0...0.....lU.....0...*.H.....0..1.0...U....US1.0...U....New Jersey1.0...U....Jersey City1.0...U....The USERTRUST Network1.0,..U...%USERTrust RSA Certification Authority0...200130000000Z..300129235959Z0K1.0...U....AT1.0...U....ZeroSSL1*0(..U...!ZeroSSL RSA Domain Secure Site CA0.."0...*.H.....0.....is~..1.#.m...T.....!.~].R|?1..l.Y8^g~KV.u..7.5Zd..L.,$..m....Mf.....!t..C..q...L8}.*.....8...N..h..kw..@...._.....=$._.d...Y..B.oPR..Z.'<.....^...T.c.....q.+{@.5.....A...F..|2E...E.e..Pt.....Vu..J..j.u...5../.]..\..;..w..%5-.V..^x$.....(g..0...mZ'...;.`.r3..}.*c...C.u.;.L..7t...>.D....B.f...tJ..."Y..bf:!...'.{...r2n..]tU.....F.....Ex;6E.....-5E*....X.....B.y9.$....g.....|..OxR..WOaU.'.8y..B...-....jG.iV'4%:KI.J.v.i.-o....."m.z.Wc..%9J.~h.i.H.@...#....Ui.(KBU.....u0..q0...U.#..0...Sy.Z.+J.T.....f.0...U.....xh...h.=r._.>....0...U.....0...U.....0.....0...U.%..0...+.....+.....0"..U. ..0.0...+.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\10BDC45B4A27319429BBC4F08A4E8A10	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	548
Entropy (8bit):	3.0821451842731133
Encrypted:	false
SSDEEP:	12:hkEY4qMUE0WYtBoxn5kEY4qMUE0WYtBoxn/:hk/4qMUE0Doh5k/4qMUE0Doh/
MD5:	F0342FB8324159FB21350893490ACB59
SHA1:	D360145D18733F377865FBFA1A9EAA3B59683D1F
SHA-256:	2ED3BDF09B8420522C5587F32BFBA4202E0932791DB8C33421689D0126435BE0
SHA-512:	EF4025CF2A7A504627D513EC7456BDE02F3CC45D9C74B4B9F585237F46E8E4BEA8FEB122EAAAFF3B89FD2F26444B5BDEBB436BA32CEC8BE030A0C7C8904B9F23
Malicious:	false
Reputation:	low
Preview:	p..... .....'_..(..... .....6....@8.....h.t.t.p.:././.z.e.r.o.s.s.l...c.r.t...s.e.c.t.i.g.o...c.o.m./.Z.e.r.o.S.S.L.R.S.A.D.o.m.a.i.n.S.e.c.u.r.e.S.i.t.e.C.A...c.r.t...".5.e.3.2.1.c.8.0.-.6.d.9."...p..... .....'_..(..... .....6....@8.....h.t.t.p.:././.z.e.r.o.s.s.l...c.r.t...s.e.c.t.i.g.o...c.o.m./.Z.e.r.o.S.S.L.R.S.A.D.o.m.a.i.n.S.e.c.u.r.e.S.i.t.e.C.A...c.r.t...".5.e.3.2.1.c.8.0.-.6.d.9."...

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\DOSBP6IX\20.37.46[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FED
Malicious:	false
Reputation:	low
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{C709F190-CB1A-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8589948561000256
Encrypted:	false
SSDEEP:	192:rFXZ6Ze2VWFtgu5fon0sMdsc2+mjDfunXcX:rFJmVsPgAxFCnb
MD5:	DE3C3390320F5A450CCBB747897B9A3C
SHA1:	8A3C61AF905FFF4D74883365EF940C9CE08EE4F0
SHA-256:	6B530EA361511F5B187AD29D9BF9141025FA69ECC7739589103972D11C43C8E2
SHA-512:	820C303F3F16C0593C38A19C9D7C6D2219BBC06EBB15BD015212E7A0F21FC8AF1216BC8F03CBCF62DC3767EF7BC6E144AE5064C898C5208493369346969645D
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\{C709F192-CB1A-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	42718
Entropy (8bit):	2.162818080885704
Encrypted:	false
SSDEEP:	192:rxXZuQWz6Mk7jR2xW4MErtM0xqkdMqipdF/MalwMgdbzM6Mth:rxJrWWxnAgdiCYq/nRL4q
MD5:	CEDCA673B505DAD3639B291110406A31
SHA1:	05E70FEDB6F4D0E8D6E314B4FC3B0AB65E9C2267
SHA-256:	6DDF732FDCFD6F440C5BC1A50122B1F95D4979E9926899ECA469F27F90680E9C
SHA-512:	59418953EF509CDABAF3D94DB666A36E1D381FFE4C1FE4703F89145A9C56B7920253D731FBA73E1C833D8529F968F6EB863F5B0A349B655B3E847E329C563142
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\{D0ED2495-CB1A-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.566420319069321
Encrypted:	false
SSDEEP:	48:IwLGcprWGwpajG4pQDGrapbSTGQpKpG7HpR9TGlpG:rRZOQV6nBStAIT7A
MD5:	5B487B78846D31E6750C6B7F0C277D27
SHA1:	9F4A9402A37AF173576350E4A795AC1E6AD29838
SHA-256:	50E78650DD6D05500C44DB47BB098B73ACCECBBB2AA36FD29707755E3FA7FF6A
SHA-512:	CC2FB3328ED7EDAB931A619F2E1A923DBDAB4720EDCFC8688BE272E4AE52D90DE4C8811ACA0A945BFA2FCAE689BB432BAF89E3E94C86E495843BB11BC391EAFD
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1890
Entropy (8bit):	6.987122291514337
Encrypted:	false
SSDEEP:	24:LIQoCtoLOEKYVe/Yv5BnC3PeFKtQO/T1WPooCtoLOEKYVe/Yv5BnC3PeFKtQO/TN:LHrW8bkKe4T1WPorW8bkKe4T1WA

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
MD5:	DF7BA455A98FC77265B73DE043467F14
SHA1:	2C1250DF0102F301BCEC530F271D519BEF4E6129
SHA-256:	080AA832B3DF9F1F6D2F725698AB2EABDBEC262F905523010853B404F9DFA093
SHA-512:	9989161885E216D2AE24973029B2E3061736C2639E5C785AE62AB28821B3BE161E007CF42CAB94C0E098775C86E889D0A37FA973979FCC8A9DE02D1F9E904D63
Malicious:	false
Reputation:	low
Preview:	8.h.t.t.p.s.:././.w.e.b.m.a.i.l...c.a.b.l.e.l.y.n.x...c.o.m./.w.e.b.m.a.i.l./.i.m.a.g.e.s./.f.a.v.i.c.o.n...i.c.o.*....PNG.....IHDR.....a....pHYs...#...#.x.?v....gAMA....|.Q.... cHRM..z%.....u0...`..:....o._.F....IDATx.b...?.%. ...(.....~M.....??..10.D...@.cD.....[..LV.?..>l.<.... .X.2....y4$N2H..g`..s.D.....)..../=...Rg`a....@L....i...u....~rb`.....\... ..h% ...1.w.....^3a.{/..._.....+.]...}.....AN\|+.._q.u.....K.....4fX.v1.'..,L.....a.....@.....@C..AC.%.....;..3.Y.....rrr`.....0..YX..m....h.....,@.(l.....)P.j.....@.....b.9.d....02.... #C.....y.v.....t!+\..h.....H....\_...O./.W7g.....C@P.....X...13..={.....@,@W0.....AIY.l .O..3P...(...._...?..\.... .X..Mr.w`puqepqufPRQ....%.$..@.A.....d...D.....@, ..|..^...v..<.../_.....*.%.....#@...m...../.....fD...Y.A....>...#... .(.....'...w6F....IEND.B`.....<..`....<..`....).h.t.t.p.s.:././.w.e.b.m.a.i.l...c.a.b.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\button_background[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 18
Category:	downloaded
Size (bytes):	146
Entropy (8bit):	4.470182862711351
Encrypted:	false
SSDEEP:	3:CHhWAGUrPUKTIWyHR/dv1ezdylXxlcg+QC6xlen:2hWAGarxY/Oz3Qxjen
MD5:	93C2060A176476CE71D13FE682CDEF80
SHA1:	7B9DF364D5793F57CEBC5631C3DDA7287F8256DD
SHA-256:	428CFFB019423578BBAD09A8B38BAA7F83E67667555EB3AF23C4D2756D4CB1F6
SHA-512:	E030A542A713AF61E9D7284C6F55C6910896BA066FDAD219C92AA2F6A621CEA461E275B64DEEEE95392FACCCFCC7834678372DDF84A68173344AB000370A1E3A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://webmail.cablelynx.com/webmail/themes/skins/24hour_one/button_background.gif
Preview:	GIF89a.....!.....,.....`.$..)Da,....2..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\magicmail[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	15238
Entropy (8bit):	5.129928008310209
Encrypted:	false
SSDEEP:	192:O/3QzYi/BIqskLXxhO3ZEvQUIJjpnwkXTG53mzUQQucVGjCb+iDYM1a1IfczE18:AQUi2BkLvQUI7nwFmz2GjCWcoT
MD5:	ECE956B0CD7D6EDE1C2778E4F0DB9632
SHA1:	1B1A1FB1C863F790D67E37B0A3F5BD402AD80E62
SHA-256:	C736AE25C8C8262E83B40846AD2B97662E26AC45AD2D390FF394C255952AB094
SHA-512:	E0E373B2B3E71A43F2100869CFF2F160A2A379E7CEDD127257B371E8CC6371F7FA0C0B2387317B9603B3B1B156E4584C3EE1B66F6FC0AA649A37C9AB9CFE444F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://20.37.46.234/ext/magicmail.css
Preview:	/* ----------.... MagicMail Server CSS (2.1).. http://magicmail.linuxmagic.com/.... Copyright: 2010 Wizard IT Services, All Rights Reserved.. All style attributes in alpha-numeric order starting from 0....---------- */..../* Quick Styles */..a {color: #10456B}..a:hov {color: #000}....h2 {...color: #10456B;...font-size: 16px;...font-weight: bold;...margin: 0 0 8px;..}....h3 {...color: #343434;...font-size: 14px;...font-weight: bold;...margin: 4px 0;..}.....minibutton {...background: #FFF;...border: 1px solid #999;...display: inline-block;...-moz-border-radius: 3px;...padding: 1px;...-webkit-border-radius: 3px;..}..... minibutton a {....background: #DEDEDE url(../pics/background-mailboxheader.gif) repeat-x;....color: #343434;....cursor: pointer;....display: block;....font-size: 11px;... .padding: 1px 6px;....text-align: center;....text-decoration: none;…white-spa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\magicmailseven_login[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop 7.0, datetime=2007:07:30 16:23:14], baseline, precision 8, 444x229, frames 3
Category:	downloaded
Size (bytes):	20132
Entropy (8bit):	6.678926693410921
Encrypted:	false
SSDEEP:	384:iEQEEqwAnP+iiiiiiiiiiHPZT3xxxxHxxxxeq:M8woP+iiiiiiiiiiHhTJ
MD5:	6B07FA541B071A7E2402115BB2E95360
SHA1:	876A06D227582788387E013C70C86A84A047A1E7
SHA-256:	8DEA0A20634B20C1A178F5B6E466450C87E3C7E6C0BF48EFC99A03329B62EE4E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\magicmailseven_login[1].jpg	
SHA-512:	FE6FCAF3AFB34D17098F5307F06660258005F5A9BD088DAEA46CEA4C6D3A5862786D1EB2EFFB4AA8175D821FEC421036234D65EAA1A254F5174202C150AE0DE E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://webmail.cablelynx.com/webmail/themes/skins/24hour_one/magicmailseven_login.jpg
Preview:	......JFIF.....H.H.....XExif..MM.*.....b.....j.(.....1.....r.2.....i.....H.....H....Adobe Photoshop 7.0.2007:07:30 16:23:14..... .....(.....&.....*.....H.....H.....JFIF.....H.H.....Adobe_CM.....Adobe.d..... .....B...."..... ?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'..... .....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?..k..Z.....i....?J..C....7..._i...! (E,....%....yB.....7..._i...!(IL....%....yB.....7..._i...!(IL....%....yB.....7..&=.....E...o...!.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\wizard[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	assembler source, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2843
Entropy (8bit):	5.161326820918581
Encrypted:	false
SSDEEP:	48:1RjomE2qy7ii2zqZArJiFnMHkzlt6b9QvpiIjQ:10mGN2Eon2k49QIv
MD5:	D06FA5B9EF680BA6898C5BAC7EB772DC
SHA1:	FCE2C710AF34FBEBFA08A7739C65C60882570C1E
SHA-256:	88D8D925E8F2A523E7D9BFCCEE791722C8A85F4DC005A6A24009453E1C8DA828
SHA-512:	F72A9336380F46515EE44D3B67027D18AABAE6E1C5B941B785CFAF01EF50F788987C1E550CC648130425D118BF226B39E7FC41FE6A435C2B5F40AF72C1CB062E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://20.37.46.234/ext/wizard.css
Preview:	/* ----------.. Wizard CSS (2.1) Framework. http://www.wizard.ca.. Copyright: 2010 Wizard IT Services, All Rights Reserved. All tyle attributes in alpha-numeric order starting from 0..---------- */../* Reset styles */.*{outline:none}a,abbr,acronym,address,blockquote,body,caption,code,dd,del,dfn,dl,dt,em,fieldset,form,div,h1,h2,h3,h4,h5,h6,html,iframe,img,label,legend,li,object,ol,p,pre,q,span,table,tbody,td,tfoot,th,thead,tr,ul{border:0;font-family:inherit;font-size:100%;font-style:inherit;font-weight:inherit;margin:0;padding:0;vertical-align:baseline}body{line-height:1.5}table{border-collapse:separate;border-spacing:0;}caption,th,td{text-align:left;font-weight:normal}table,td,th{vertical-align:middle}a{cursor:pointer}a img{border:none}blockquote:before,blockquote:after,q:before,q:after{content:""}blockquote,q{quotes:"" ""}../* Quick styles */..left { float: left;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\24hour_one[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	36178
Entropy (8bit):	5.295297840942487
Encrypted:	false
SSDEEP:	384:z1oydgQFHExkNXdoZF19DgT32jrtbZAJ3MR2u7HMrGhbYuJbWUv0YVlbPl:xoydjNvdoZP9DgTE9Iu7HXJ5789b9
MD5:	F4ED07A4F6C14E234DF00EDEA1C24B1C
SHA1:	0A3008E39EFE6D3DCE2F71E01956C67D181CC197
SHA-256:	70FFA31E8EDA59725FB34F1B2DF39E604653A56BC477EF19F0CCCED4ED2FC455
SHA-512:	270EA88936C26A1F1E0732D8A090E3C42E6316BF6DB9CADDEFDDDECEC27D23A046F17C4481F33FD6F22AA56B59FE9A87A23B5AA9E824A4D75AA26999D1B5F B8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://20.37.46.234/ext/24hour_one.css
Preview:	/*. * Cascading Style Sheet (CSS 467) for MagicMail Seven (Default MagicMail Webmail Theme). * Author: Evgueni Naverniouk, evgueni@linuxmagic.com, http://www.linuxmagic.com/. * COPYRIGHT INFORMATION - DO NOT REMOVE. * Copyright (c) 2007 LinuxMagic Inc. All Rights Reserved.. *. * All style attributes in alpha-numeric order starting from 0. */ ../* . * ========== =. * Global Elements and General Styles. * ========== =====. */. .html, body{..color: #000;..font-family: Verdana, Arial, Helvetica, Tahoma, sans-serif;..font-size: 11px;..margin: 0;..padding: 0;..text-decoration: none;..}../* Left Frame */.body.left {..background: #2971B5 url('https://webmail.cablelynx.com/webmail/themes/skins/24hour_one/background-sidebar.gif') no-repeat left 110px;..text-align: center; /* IE Fix */.}../* Right Frame */.body.right {..background: #FFF url('https://webmail.cablelynx.com/webmail/themes/skins/24hour_one/background-topheader.gif') repeat-x; /* IE F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\home[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	5126
Entropy (8bit):	5.219023137451855
Encrypted:	false
SSDEEP:	96:l1g3QYGOcZhfSXGh4g/hpYKavs/HGISeB:AQYGBZhfS2hNgs/ai
MD5:	4AAA2E5849E692B91C549824712DE00C
SHA1:	B445778FE2FB60CD2773A410C4C139FAAE28A510

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\home[1].htm	
SHA-256:	2B327398DEBF0F2C1451EFA8D0FC45F1DE11E9531F09781D520931ADBD9B680A
SHA-512:	FC9D26F691A6D82900A5D475B0AB17C3ED00D662AE03F38BA09E2BA44C59108B509643E613ACF5D7D2194B0C4BF72BAFE325977D7A8C7DB0D1AAB125A949BE61
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\home[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://20.37.46.234/home?ids=38342e31372e35322e3138&email=sharcup@wickersmith.com
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">..<html><head>..<meta http-equiv="content-type" content="text/html; charset=UTF-8">..<meta name="robots" content="noindex,nofollow">..<meta http-equiv="X-UA-Compatible" content="IE=8">..<link rel="stylesheet" type="text/css" href="ext/wizard.css"><link rel="stylesheet" type="text/css" href="ext/magicmail.css"><link rel="stylesheet" type="text/css" href="ext/magicmail_standard.css"><link rel="stylesheet" type="text/css" href="ext/magicmail_003.css"><link rel="stylesheet" type="text/css" href="ext/magicmail_002.css"><link rel="stylesheet" type="text/css" href="ext/webmail_options.css"> [if IE 8]>..<link rel="stylesheet" type="text/css" media="all" href="/webmail/src/ie8.css?v=3.0.0-8"><![endif]-->..<script type="text/javascript" language="JavaScript">.. ..if (self != top) { try { if (document.domain != top.document.domain) { throw "Clickjacking security violation! Please log out immediately!"; /* this code should never

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\htmlcanvas[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	60482
Entropy (8bit):	5.043235520441017
Encrypted:	false
SSDEEP:	768:AqnFRkv6Hbz4DaYBHBzRzQsh8k7pk8B0SjPI4/HlD7J+NIAXuT:AmyvUbzYHBVMyk8DI4/HV7J+NIAXI
MD5:	8A6C3B82B3AAA5BD936A7A707445604B
SHA1:	CA0A87AF38787C875BD39211D3C1A7B6074214C8
SHA-256:	AA845AEF7DBCE9995DE9FE43B9246EC55E8242545D9EBCEC87400667B167EAF0
SHA-512:	BFB8088903F0E6830F526519E26BD338E2BFEE544AB3045C43E2440981D5D1FE56FEECCB3BBFE48F9EBE6775CC88ACB79E03A6BC55317B46F51E298B45859299
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://20.37.46.234/ext/htmlcanvas.js
Preview:	/*.* Fingerprintjs2 1.5.1 - Modern & flexible browser fingerprint library v2.* https://github.com/Valve/fingerprintjs2.* Copyright (c) 2015 Valentin Vasilyev (valentin.va silyev@outlook.com).* Licensed under the MIT (http://www.opensource.org/licenses/mit-license.php) license..*.* THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS".* AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE.* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.* ARE DISCLAIMED. IN NO EVENT SHALL VALENTIN VASILYEV BE LIABLE FOR ANY.* DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES.* (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SU BSTITUTE GOODS OR SERVICES;.* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND.* ON ANY THEORY OF LIABI LITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT.* (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF.* THIS SOFTWARE, EVEN IF ADVISED

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\magicmail_002[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	assembler source, ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	7995
Entropy (8bit):	4.995319677467021
Encrypted:	false
SSDEEP:	96:mjl1O1q40/kcaQdhI48/sXp+XUX5QtCOcXA6qiQ4z2IsuBpH+FL:mp1O1dcfd5+kpQtCOdiXz2+ROL
MD5:	3435D888D0DC6AA6AA9457452B4A1A88
SHA1:	DECFC4F59B1633EFF5C9EC2596C7391D722354F8
SHA-256:	5FCB6EDCAB23F49888DCA399DA9372D69020F4AEE6C8176888D7B77ABE8AC84D
SHA-512:	747A4943C1894B5566F8726968A8E7D8C0F0F0C44990ABB3D92CA327E0A4CD86ED4F6BA535B48B962876467A1E0ECA3245F61541E984C778520F29A4608D1120
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://20.37.46.234/ext/magicmail_002.css
Preview:	/* ----------....MagicMail Server CSS (2.1)..Component: Email Options..http://magicmail.linuxmagic.com/....Copyright: 2010-2013 izard IT Services, All Rights Reserved..All style attributes in alpha-numeric order starting from 0....---------- */....#EmailOptions { line-height: 150%;.. margin: 0 8px 0 auto;.. width: 100%;..}..../* Webmail Rewrite */...right {float: none;}...right #EmailOptions {float: none; margin: 10px; width: 750px; }...right .Aliases .minibutton {display: none;}....#EmailOptions table.MagicDataTable td.success,..#EmailOptions table td.error {.. padding: 8px;..}....#EmailOptions . Description {.. color: #343434;.. margin: 8px;.. padding: 0;.. text-align: justify;.. width: auto;..}....#EmailOptions table {.. background: #F9F9F9 url(../pics/b ackground-mailbox.gif) repeat-x;.. border: 1px solid #999;.. border-spacin

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	810
Entropy (8bit):	7.247123950802036

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\favicon[1].ico	
Encrypted:	false
SSDEEP:	12:6v/7OXYmAAWntoLLlvvICRFKwvCOrPm/Y80b4Q5Yfun9w3aSfeFgXtQRo/T18w7K:nCtoLOEKYVe/Yv5BnC3PeFKtQO/T1WL
MD5:	2BA9B777483DA0A6A8B29C4AB39A10B2
SHA1:	1752AA117DB45034EF973108610439789BE614AE
SHA-256:	935A19A7C36B6E6D8233C432FD739AF302E516912560018288EB8769E09CE37F
SHA-512:	5303833EECD4BE57E619379C8A432E7C4AB96DA47043A8FD692AD5FB54AD656396F98A05C8F83F69F58778AEE5E4138BECD3B707088AFF6CF8C38B81A1D8896
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://webmail.cablelynx.com/webmail/images/favicon.ico
Preview:	.PNG.....IHDR.....a....pHYs...#...#.x.?v....gAMA....|.Q.... cHRM..z%.....u0...`..:....o._.F....IDATx.b...?.%. ...(.....~M.....??..10.D...@.cD.....[..LV.?..>I.<.... .X.2....y4$N2H..g`..s.D.....)..../=...Rg`a....@L....i...u....~rb`.....\... ..h%...1.w.....^3a.{/..._.....+.]...}.....AN\|+.._q.u.....K.....4fX.v1.'.,L.....a.....@.....@C..AC. %.....;..3.Y.....rrr`.....0..YX..m....h.....,@.(l.....)P.j.....@.....b.9.d....02.....#C.....y.v.....t!+\..h.....H....\_...O./.W7g.....C@P.....X...13..={.....@,@W0.....AIY.I .O..3P...(....._...?..\.... .X..Mr.w`puqepqufPRQ....%.$..@.A.....d...D.....@,..|..^...v..<.../_.....*.%.....#@...m...../.....fD...Y.A....>...#... .(....'...w6F....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\favicon[2].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	810
Entropy (8bit):	7.247123950802036
Encrypted:	false
SSDEEP:	12:6v/7OXYmAAWntoLLlvvICRFKwvCOrPm/Y80b4Q5Yfun9w3aSfeFgXtQRo/T18w7K:nCtoLOEKYVe/Yv5BnC3PeFKtQO/T1WL
MD5:	2BA9B777483DA0A6A8B29C4AB39A10B2
SHA1:	1752AA117DB45034EF973108610439789BE614AE
SHA-256:	935A19A7C36B6E6D8233C432FD739AF302E516912560018288EB8769E09CE37F
SHA-512:	5303833EECD4BE57E619379C8A432E7C4AB96DA47043A8FD692AD5FB54AD656396F98A05C8F83F69F58778AEE5E4138BECD3B707088AFF6CF8C38B81A1D8896
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://webmail.cablelynx.com/favicon.ico
Preview:	.PNG.....IHDR.....a....pHYs...#...#.x.?v....gAMA....|.Q.... cHRM..z%.....u0...`..:....o._.F....IDATx.b...?.%. ...(.....~M.....??..10.D...@.cD.....[..LV.?..>I.<.... .X.2....y4$N2H..g`..s.D.....)..../=...Rg`a....@L....i...u....~rb`.....\... ..h%...1.w.....^3a.{/..._.....+.]...}.....AN\|+.._q.u.....K.....4fX.v1.'.,L.....a.....@.....@C..AC. %.....;..3.Y.....rrr`.....0..YX..m....h.....,@.(l.....)P.j.....@.....b.9.d....02.....#C.....y.v.....t!+\..h.....H....\_...O./.W7g.....C@P.....X...13..={.....@,@W0.....AIY.I .O..3P...(....._...?..\.... .X..Mr.w`puqepqufPRQ....%.$..@.A.....d...D.....@,..|..^...v..<.../_.....*.%.....#@...m...../.....fD...Y.A....>...#... .(....'...w6F....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\magicmail_standard[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	10225
Entropy (8bit):	5.133676394566873
Encrypted:	false
SSDEEP:	192:HHQeHBeYqo/tBURs4LumlSXtqJkwoFA7GMRFA7GUh:nQseYZFn4LsA+FhWFhA
MD5:	C36A84E59BBCC82E4FFF46CBE6200D40
SHA1:	2F278B77CA948E836CC9C0D68B4F1D4078C3D4C8
SHA-256:	5C793EC0B65DA57C1A7F63EAE777447D946963167A59E3D3535D0E0BDAF2CCE3
SHA-512:	F0C920B6336F56E7AD6BF64926E8D20B276BA4AF8BFDC126224FCC18CF695EA2E30779F855BF52F8DE792C47E7C49106C5BE0130DA69A8FC61E1541A15F06C7E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://20.37.46.234/ext/magicmail_standard.css
Preview:	/*. * COPYRIGHT INFORMATION - DO NOT REMOVE. *. * This file is part of the MagicMail (TM) Project and is. * Copyright (c) LinuxMagic Inc. 2010-2018 All Rights Reserved. *. * This file contains Original Code as created by LinuxMagic Inc.. *. * The Original Code is distributed on an 'AS IS' basis,. * WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, AND LINUXMAGIC. * HEREBY DISCLAIMS ALL SUCH WARRANTIES, INCLUDING WITHOUT LIMITATION, ANY. * WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, QUIET. * ENJOYMENT OR NON-INFRINGEMENT.. *. * Do NOT download, distribute, use or alter this software or file in any. * way without express written permission from LinuxMagic Inc. or its parent. * company Wizard Tower TechnoServices signed by an authorized company officer.. *. * Author(s): Anonymous. * William Storey <william@linuxmagic.com>. *. * $Id: magicmail.css 28715 2018-05-17 15:32:44Z shaun $. */* ----------

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\webmail_options[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	3831
Entropy (8bit):	4.9282778014029445
Encrypted:	false
SSDEEP:	96:kCIFCSbCk+aCrChaCcRwCRYC5vpjChC4entu+CnC/jPCclvbCvQCWCunLFnPFnyh:I+LVNtfy

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\webmail_options[1].css	
MD5:	9919710117F9B222DAF7D357BC8F1FF0
SHA1:	6C865B889DAAFD611708DD4696C6E44ECFA7E653
SHA-256:	163252D1DCD6F955FF6A4892FD8F5137CA0A71370D994EA406A246B722002DBE
SHA-512:	5BCD215FC13A50521F367E9DD8BAA4723E39C950EF731A5FF2AF23D0FD7544E694AE4C6B08A29FBC3F3F94DA4E3F6D150D4799A9D90BA4AC85A2D0308DBC89 52
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://20.37.46.234/ext/webmail_options.css
Preview:	/*. * ============================. * Options Pages. * ============================. */./* copied from abook2_opt.css */.#AbookOptions {. line-height: 150%;. margin: 0 8px 0 auto;.}../* Webmail Rewrite */..right {float: none;}..right #AbookOptions {float: none; margin: 10px;}..right .Aliases .minibutton {display: none;} ...width-750 {. width: 750px;.}..#AbookOptions table.MagicDataTable td.success,.#AbookOptions table td.error {. padding: 8px;.}..#AbookOptions .Description {. color: #343434;. margin: 8px;. padding: 0;. text-align: justify;. width: auto;.}..#AbookOptions table {. background: #F9F9F9 url(../../../pics/background-mailbox.gif) repeat-x;. border: 1px solid #999;. border-spacing: 0;. margin: 0 auto 8px !important;. -moz-border-radius: 4px;. padding: 0;. -webkit-border-radius: 4px;. wid th: 98% !important;. border-radius: 4px;.}..#AbookOptions table.optionsmenu {. background-image: none;. background-color: transpare

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\magicmail_003[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	5289
Entropy (8bit):	5.062822816179364
Encrypted:	false
SSDEEP:	48:+2CybymDxFhm9JOmoelyerVJLJfY12ajkJ7doySpsqpoyJoGEQAEMvpVrF0owJQ1:++VfqJJldJlfYr6BT/oJnskQ
MD5:	F92D41DBD289A81C6A52FC602FAA6C2A
SHA1:	7C68CE2B4F3D12D999B0BEC7CD86F1858B07689C
SHA-256:	45060273007B046913570FB3F9F0D552A2107ACA1B377331497018EF432C8ADF
SHA-512:	BA554E111C8F5E7143995A7A5484C0A68E1A13281A7F02E51E0E83578F89AF07266F471CE8FD9424373D9DF5BF0EF026A2AB6FF8F7779B832824C9E1AA8F3A8B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://20.37.46.234/ext/magicmail_003.css
Preview:	/* ----------.... MagicMail Server CSS (2.1).. Component: Spam Management.. http://magicmail.linuxmagic.com/.... Copyright: 20 Wizard IT Services, All Rights Reserved.. All style attributes in alpha-numeric order starting from 0....---------- */..../* Webmail Rewrites */...right {float: none}..#signout_button {text-align: right}..#spam_form {padding-left: 15px;}..#spam_form .SpamManagement {margin: 10px 0 0}.....SpamHeader {margin: 0 0 6px}.....SpamError.success, .SpamError.error {width: 590px}.....SpamManagement {width: 600px}.....AntiSpamProtection {....margin: 0 0 8px 0;....position: relative;....width: 100%;...}.....AntiSpamProtection h2 {....font-size: 16px;....text-align: left;...}....AntiSpamProtection h3 {....font-size: 14px;....text-align: left;...}.....CustomRul e {....border: 1px solid #CECECE;....border-bottom: 0;...}....BlockSpot {....border: 1px s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\security.en[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	2662
Entropy (8bit):	4.933596587735419
Encrypted:	false
SSDEEP:	48:hjht9F71fN9e9DY/Z+09T9xMeva9lZF2aj9TwCez6N1H+BaVGFC8W:hjr9R1F9e9Y/l09T9xMeS9D4aj96z6DN
MD5:	11C71CFF26CD0F68A05AA85D9AE9E3ED
SHA1:	3FB8B8216080B427A07A0E0CB4225D1465E419C5
SHA-256:	C6D8F0BF8B1EDBEBFFC4E36D367D7537C13A43F46A24296C297B465C0DE7587F
SHA-512:	7248E8217C95808718F48A0989C7CF61249C77C2D035D1D4C786BA3C25D34BC801E8BCCFA1FCE07B21A6F942E3005E0FB9260D49180434AF04DE294B980EBAC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://webmail.cablelynx.com/webmail/plugins/login_auto/security.en.php
Preview:	<HTML>. <HEAD>.<TITLE>MagicMail WebMail Interface - Security Notice</TITLE>.</HEAD>.<BODY>. .<TABLE BGCOLOR="FFFFFF" BORDER="0" CO LS="1" WIDTH="90%" CELLSPACING="0" .CELLPADDING="2" ALIGN="CENTER">. <TR>. <TD>..What does "Remember my.Name" .mean?... </TD>. </TR>. <TR>. <TD>.When you sign in with your name,.your browser can "remember" this information. Check the box.and you won't have to enter this information each time you come back..If you don't log in for.7 days, this information will be "forgotten".. </TD>. </TR>. <TR>. <TD>.. Should I be concerned about security?. </TD>. </TR>. <TR>. <TD>.If you are concerned that other people might.attempt to access your email account, do not check the "Remember my.Name" box.. You may want to click "Sign Out" when you leave your computer, which ensures.that you will be asked for your login information the next time anyone .accesses this webmail from your computer.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\sharcup@wickersmith[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	111
Entropy (8bit):	4.887381944244238
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\sharcup@wickersmith[1].htm

SSDEEP:	3:gnkAqRAdu6/GY7voOkADFoHDJoXWRIOPSvoaeYLn:7AqJm7+mmHSXWRINo7YL
MD5:	0212C36A28F83332821064318486217E
SHA1:	EB449500D512A3C8DB5E2FAC4FC8945BF292D1D5
SHA-256:	E035F591EC88B043F2974ABC5E996AE5A2FB6D1F963B83A8D43852D3402A23A2
SHA-512:	D866D7D3104E2FF3EAE585994F3578C85D1662BDC511C30F0F64162073B4ADED7FF0BE7A873DC75AA0F77C5EEB6D12F7AEB5BE1BD9B38B0E5C399FF9F4C6D BC
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Phisher_2, Description: Yara detected Phisher, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\sharcup@wickersmith[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://blockstyerts.live/sharcup@wickersmith.com
Preview:	<script type="text/javascript">window.location.href = "https://20.37.46.234/?sharcup@wickersmith.com"</script>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\wickersmith[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 128 x 99, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	16448
Entropy (8bit):	7.979292700486458
Encrypted:	false
SSDEEP:	384:zAu6XeFTm2L+cEi/WZK+01HHZoQV6P6CosDBacfIVnVDivLu:zA+TmJcWZKX1HHP6IsD9IDWi
MD5:	4872739EE6B376B8678430AD5F0571CC
SHA1:	BA19A5AB2AE9E80B7A7A0F48DECD721BF7DC2078
SHA-256:	7F79DC07B78D07962584D303CA8D6BB95EBF9331DB149EDB94ACC1B8A7B2552C
SHA-512:	741B9446DD204000D30D4692E22CBC346A678543C5601FE55006B6507E18A7C97EED7B74BB7CDAB5A4D543A59C5419A3EE49FD1B8A198A1D315C6AB04989A16
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://logo.clearbit.com/wickersmith.com
Preview:	.PNG........IHDR.......c.....S.....@.IDATx..y.f.Y..;w.......[j-....edlcG"v.....m<<.......Hf........dB...x..<01`<vL...<...dIn-.V........[.~.<.=..{.[.X.,..VU}.].y........8<.8...q...+..x...Ew.4..6.(D.... ..`.....8...?.._.z..\./O.s.y.1\kp.7q....<.i[X[....t..cH...M.+~G".K.>.a..,p..7......&=.x/q.........].gO..=.......y|.s.{.i`./:.C^.'.3f`w....>.N.K....T`..L.a.`...4a.&... Sw0.sq.I.......i..Y....oo..x:q.: ...G...4.Tk0c...!.czNz.DMR.B<%..NON..L.C.lX~.F...@}.'L..p2F.$..jp.JF+,}6u..e.0,.a.#d.w..m.v*.}"..0..f...$...#..54.-.Ez0....Y.y.9y.#..0Qk4Q..a..,.......l.4L"P.sV..q..+.0LZlq^....3.A H.j...Z.?...O.T..[..`0...a;5.<..#.IL.......f....<..V..d..J....9,.$..r.,......T/(..L/*..iwJ'\..8...xL.A.!>g....q@2..EP...~..br..L..O.@[..{M"..b.84l.B.^E.^.m;0M...3%..) 8...BJ.hD.RX*.bE.....78 ..%.......s.$.....~.....^.(.1N.*.@.d.I.D.....,.0.u.@.....^........b4..1u=4*U"F.Y.%&.E)&s.b.....W7.0..1.l.g.ee.J..PRa......./.v~J..4F.......\Z.t..q..'..D.T..I.u....gI..3..$. ..2.^..s;..G.bq

C:\Users\user\AppData\Local\Temp\~DF41EADA43E19DE92D.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.48090193440291656
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loAtF9loAn9lWAIOxkIyxktgkttrarY:kBqoIAIA2AIOxkIyxktgkttmU
MD5:	C0BE79DB8CB1B5F0719B32E4642BF00D
SHA1:	47567ECFB2907ACF42D4B3FF16E7510CEA664491
SHA-256:	D885074904FAC0344D278F5FD0B0FD0DDB5738D9E4FB84CB71EFC15F5D31A502
SHA-512:	35DB4AB418E4D76379B078B240C4CEA5C5C5FCAFAF2EEFA14D20E689C52FAB8C5634BDE7D3770A764B5938147D29EE92E45789C5A24BF341BF7CA10779AF74 D7
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(................... ....*%..H..M..{y..+.0...(................... ....

C:\Users\user\AppData\Local\Temp\~DF50C611A7B24C2A09.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	50713
Entropy (8bit):	0.7386841616408185
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS++4y7onKFKBTGtHaDtvOYrs72nHaDtvOYrs72/jMSAM:kBqoxKAuqR++4y7onu6qIKjMSAM
MD5:	A4FB201C537EC06A4FD8AF5F089A1069
SHA1:	DB142098141C4341C043C834E5461F09DEBAF2F5
SHA-256:	283FC6EF12D195623F01D60F968D80E507624557FCB163D80C8DBAC240024694

C:\Users\user\AppData\Local\Temp\~DF50C611A7B24C2A09.TMP	
SHA-512:	4C355B051CB12D9BE8092D92831622095BC7CFA5DAEFD35FB48BD421A1AEC9420414EE34641F406CB1641F78E98415F43A06FB5182C5C744B18330C4D0CF409
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF5806896016F953CF.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.3531252288471772
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laABzZ93LroES:kBqoxxJhHWSVSEablr
MD5:	06B7B166590EAE3AB721374E407BEF1F
SHA1:	CDAFEA8456F92DED87F56E60F548B4EDE9FB7F3D
SHA-256:	77F0460EC4E1E61B4DC9B7B9C2129341D8A1528EB4501227607757841A15D8AF
SHA-512:	583DC14C2B5D1A49DE57753346FACE670466D2B4B5C0753A5ECDE9DFD0C1D3DBD8F63A174FBAB832792EAA7C00EFB00C0148A36E455A81C5BD854091DBFC4 8B
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 18:08:15.594000101 CEST	192.168.2.3	8.8.8.8	0x160	Standard query (0)	blockstyerts.live	A (IP address)	IN (0x0001)
Jun 11, 2021 18:08:17.744077921 CEST	192.168.2.3	8.8.8.8	0x90bb	Standard query (0)	zerossl.cr t.sectigo.com	A (IP address)	IN (0x0001)
Jun 11, 2021 18:08:21.720462084 CEST	192.168.2.3	8.8.8.8	0x308b	Standard query (0)	logo.clearbit.com	A (IP address)	IN (0x0001)
Jun 11, 2021 18:08:24.789565086 CEST	192.168.2.3	8.8.8.8	0x2667	Standard query (0)	webmail.ca blelynx.com	A (IP address)	IN (0x0001)
Jun 11, 2021 18:08:33.737683058 CEST	192.168.2.3	8.8.8.8	0x2af8	Standard query (0)	webmail.ca blelynx.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 18:08:15.658694983 CEST	8.8.8.8	192.168.2.3	0x160	No error (0)	blockstyerts.live		52.161.162.59	A (IP address)	IN (0x0001)
Jun 11, 2021 18:08:17.806396008 CEST	8.8.8.8	192.168.2.3	0x90bb	No error (0)	zerossl.crt.sectigo.com	crt.sectigo.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 18:08:17.806396008 CEST	8.8.8.8	192.168.2.3	0x90bb	No error (0)	crt.sectigo.com		91.199.212.52	A (IP address)	IN (0x0001)
Jun 11, 2021 18:08:21.784641027 CEST	8.8.8.8	192.168.2.3	0x308b	No error (0)	logo.clearbit.com	d26p066pn2w0s0.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 18:08:21.784641027 CEST	8.8.8.8	192.168.2.3	0x308b	No error (0)	d26p066pn2w0s0.cloudfront.net		13.32.25.43	A (IP address)	IN (0x0001)
Jun 11, 2021 18:08:21.784641027 CEST	8.8.8.8	192.168.2.3	0x308b	No error (0)	d26p066pn2w0s0.cloudfront.net		13.32.25.101	A (IP address)	IN (0x0001)
Jun 11, 2021 18:08:21.784641027 CEST	8.8.8.8	192.168.2.3	0x308b	No error (0)	d26p066pn2w0s0.cloudfront.net		13.32.25.80	A (IP address)	IN (0x0001)
Jun 11, 2021 18:08:21.784641027 CEST	8.8.8.8	192.168.2.3	0x308b	No error (0)	d26p066pn2w0s0.cloudfront.net		13.32.25.60	A (IP address)	IN (0x0001)
Jun 11, 2021 18:08:24.970567942 CEST	8.8.8.8	192.168.2.3	0x2667	No error (0)	webmail.cablelynx.com	pop.cablelynx.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 18:08:24.970567942 CEST	8.8.8.8	192.168.2.3	0x2667	No error (0)	pop.cablelynx.com		69.60.184.109	A (IP address)	IN (0x0001)
Jun 11, 2021 18:08:33.920479059 CEST	8.8.8.8	192.168.2.3	0x2af8	No error (0)	webmail.cablelynx.com	pop.cablelynx.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 18:08:33.920479059 CEST	8.8.8.8	192.168.2.3	0x2af8	No error (0)	pop.cablelynx.com		69.60.184.109	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- blockstyerts.live
- zerossl.crt.sectigo.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49712	52.161.162.59	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 18:08:15.843461990 CEST	1373	OUT	GET /sharcup@wickersmith.com HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: blockstyerts.live Connection: Keep-Alive
Jun 11, 2021 18:08:16.647537947 CEST	1387	IN	HTTP/1.1 200 OK Date: Fri, 11 Jun 2021 16:08:14 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.3.11 X-Powered-By: PHP/7.3.11 Content-Length: 111 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 20 3d 20 22 68 74 74 70 73 3a 2f 2f 32 30 2e 33 37 2e 34 36 2e 32 33 34 2f 3f 73 68 61 72 63 75 70 40 77 69 63 6b 65 72 73 6d 69 74 68 2e 63 6f 6d 22 3c 2f 73 63 72 69 70 74 3e 0a Data Ascii: <script type="text/javascript">window.location.href = "https://20.37.46.234/?sharcup@wickersmith.com"</script>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49717	91.199.212.52	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 18:08:17.872800112 CEST	1404	OUT	GET /ZeroSSLRSADomainSecureSiteCA.crt HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Microsoft-CryptoAPI/10.0 Host: zerossl.crt.sectigo.com
Jun 11, 2021 18:08:17.935313940 CEST	1406	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 11 Jun 2021 16:08:17 GMT Content-Type: application/pkix-cert Content-Length: 1753 Connection: keep-alive Last-Modified: Thu, 30 Jan 2020 00:00:00 GMT ETag: "5e321c80-6d9" X-CCACDN-Mirror-ID: sscrl2 Cache-Control: max-age=14400, s-maxage=3600 X-CCACDN-Proxy-ID: mcdpinlb2 X-Frame-Options: SAMEORIGIN Accept-Ranges: bytes Data Raw: 30 82 06 d5 30 82 04 bd a0 03 02 01 02 02 10 6c 55 ab db d0 07 92 c7 9d 07 0c d8 11 9e d6 bf 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0c 05 00 30 81 88 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 13 30 11 06 03 55 04 08 13 0a 4e 65 77 20 4a 65 72 73 65 79 31 14 30 12 06 03 55 04 07 13 0b 4a 65 72 73 65 79 20 43 69 74 79 31 1e 30 1c 06 03 55 04 0a 13 15 54 68 65 20 55 53 45 52 54 52 55 53 54 20 4e 65 74 77 6f 72 6b 31 2e 30 2c 06 03 55 04 03 13 25 55 53 45 52 54 72 75 73 74 20 52 53 41 20 43 65 72 74 69 66 69 63 61 74 69 6f 6e 20 41 75 74 68 6f 72 69 74 79 30 1e 17 0d 32 30 30 31 33 30 30 30 30 30 30 30 5a 17 0d 33 30 30 31 32 39 32 33 35 39 35 39 5a 30 4b 31 0b 30 09 06 03 55 04 06 13 02 41 54 31 10 30 0e 06 03 55 04 0a 13 07 5a 65 72 6f 53 53 4c 31 2a 30 28 06 03 55 04 03 13 21 5a 65 72 6f 53 53 4c 20 52 53 41 20 44 6f 6d 61 69 6e 20 53 65 63 75 72 65 20 53 69 74 65 20 43 41 30 82 02 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 82 02 0f 00 30 82 02 0a 02 82 02 01 00 86 69 73 7e a3 b5 31 d8 23 e1 6d dd a4 13 d3 54 15 f5 02 eb dc 03 21 b5 7e 5d 1d 52 7c 3f 31 eb 9e 09 6c d1 59 38 5e 67 7e 4b 56 8f 75 90 b2 37 0c 35 5a 64 a5 be 4c 10 2c 24 18 c4 6d 89 8c c1 c5 92 4d 66 02 83 9d f7 e1 21 74 f9 cb 43 02 c1 71 b1 7f ab 4c 38 7d 91 2a c6 ff 89 a9 e8 e4 a1 b9 b2 da 10 85 09 89 9a 38 b7 ce f7 4e e4 9d d1 68 f9 0d 6b 77 0e da 40 1b c4 f7 e6 5f ef fb 1a cd f2 e6 fc 3d 24 a8 5f 95 64 83 0f a3 59 fe 0a 42 d3 6f 50 52 c3 ab c9 85 5a 15 27 3c be a3 1c 00 03 5e 9b ec e2 54 cd 63 03 ad c7 dc 90 b5 ba 71 c1 2b 7b 40 96 35 f8 80 ab 99 12 41 e8 1b 8a 46 df e3 7c 32 45 f4 9b 1c 45 05 65 1c 8c 50 74 a0 09 97 ba 1a 56 75 e0 0e 4a ad 93 6a 9d 75 dd e4 08 35 dd ef 88 2f f3 5d c6 f7 5c fb 0a 3b 06 c8 9f 77 a0 92 25 35 2d d4 80 56 c3 e9 5e 78 24 c8 19 de b4 a6 a2 d6 1b cf df 28 67 15 fb 30 a6 ed 0a 6d 5a 27 fa be 85 3b f6 60 ad 72 33 1a e7 7d c8 9e 2a 63 98 05 b1 43 86 75 b9 3b a4 4c 03 bd 37 74 12 bd da 3e 97 44 dd 84 b6 d2 e4 42 eb a3 66 0c be 8d 74 4a b5 a5 8c 22 59 0d 91 62 66 3a 21 e6 12 b4 27 80 7b ed 88 d9 08 72 32 6e 9a ad 5d 74 55 f8 89 a4 c8 e3 46 ba ce 0b c8 06 dc 45 78 3b 36 45 f7 1a 1f bd de af b7 2d 35 45 2a 81 04 f9 ac 58 09 84 c9 85 c7 be ab 42 00 79 39 95 24 a1 d6 f9 93 67 b1 ec ff 86 bb 82 7c e9 b4 b5 e7 4f 78 52 e6 1c 57 4f 61 55 e9 27 99 38 79 13 1f 42 04 a8 a9 2d 2d 96 db 02 81 6a 47 fe 69 56 27 34 25 3a 4b 49 c0 4a ab 76 c6 b6 69 18 2d 6f ee fe 83 86 e7 a9 cb 22 6d 9f 7a 92 57 63 e8 06 25 39 4a a9 7e 68 04 69 c1 48 9b 40 c1 a6 e3 88 23 c8 d0 ea 0e 55 69 f9 28 4b 42 55 07 f7 1f 02 03 01 00 01 a3 82 01 75 30 82 01 71 30 1f 06 03 55 1d 23 04 18 30 16 80 14 53 79 bf 5a aa 2b 4a cf 54 80 e1 d8 9b c0 9d f2 b2 03 66 cb 30 1d 06 03 55 1d 0e 04 16 04 14 c8 d9 78 68 a2 d9 19 68 d5 3d 72 de 5f 0a 3e dc b5 86 86 a6 30 0e 06 03 55 1d 0f 01 01 ff 04 04 03 02 01 86 30 12 06 03 55 1d 13 01 01 ff 04 08 30 06 01 01 ff 02 01 00 30 1d 06 03 55 1d 25 04 16 30 Data Ascii: 00lU0*H010UUS10UNew Jersey10UJersey City10UThe USERTRUST Network1.0,U%USERTrust RSA Certification Authority0200130000000Z300129235959Z0K10UAT10UZeroSSL1*0(U!ZeroSSL RSA Domain Secure Site CA0"0*H0is~1#mT!~]R|?1lY8^g~KVu75ZdL,$mMf!tCqL8}*8Nhkw@_=$_dYBoPRZ'<^Tcq+{@5AF|2EEePtVuJju5/]\;w%5-V^x$(g0mZ';`r3}*cCu;L7t>DBftJ"Ybf:!'{r2n]tUFEx;6E-5E*XBy9$g|OxRWOaU'8yB--jGiV'4%:KIJvi-o"mzWc%9J~hiH@ #Ui(KBUu0q0U#0SyZ+JTf0Uxhh=r_>0U0U00U%0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49718	91.199.212.52	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 18:08:17.887037039 CEST	1404	OUT	GET /ZeroSSLRSADomainSecureSiteCA.crt HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Microsoft-CryptoAPI/10.0 Host: zerossl.crt.sectigo.com

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 18:08:17.949826002 CEST	1408	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 11 Jun 2021 16:08:17 GMT Content-Type: application/pkix-cert Content-Length: 1753 Connection: keep-alive Last-Modified: Thu, 30 Jan 2020 00:00:00 GMT ETag: "5e321c80-6d9" X-CCACDN-Mirror-ID: sscrl2 Cache-Control: max-age=14400, s-maxage=3600 X-CCACDN-Proxy-ID: mcdpinlb5 X-Frame-Options: SAMEORIGIN Accept-Ranges: bytes Data Raw: 30 82 06 d5 30 82 04 bd a0 03 02 01 02 02 10 6c 55 ab db d0 07 92 c7 9d 07 0c d8 11 9e d6 bf 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0c 05 00 30 81 88 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 13 30 11 06 03 55 04 08 13 0a 4e 65 77 20 4a 65 72 73 65 79 31 14 30 12 06 03 55 04 07 13 0b 4a 65 72 73 65 79 20 43 69 74 79 31 1e 30 1c 06 03 55 04 0a 13 15 54 68 65 20 55 53 45 52 54 52 55 53 54 20 4e 65 74 77 6f 72 6b 31 2e 30 2c 06 03 55 04 03 13 25 55 53 45 52 54 72 75 73 74 20 52 53 41 20 43 65 72 74 69 66 69 63 61 74 69 6f 6e 20 41 75 74 68 6f 72 69 74 79 30 1e 17 0d 32 30 30 31 33 30 30 30 30 30 30 30 5a 17 0d 33 30 30 31 32 39 32 33 35 39 35 39 5a 30 4b 31 0b 30 09 06 03 55 04 06 13 02 41 54 31 10 30 0e 06 03 55 04 0a 13 07 5a 65 72 6f 53 53 4c 31 2a 30 28 06 03 55 04 03 13 21 5a 65 72 6f 53 53 4c 20 52 53 41 20 44 6f 6d 61 69 6e 20 53 65 63 75 72 65 20 53 69 74 65 20 43 41 30 82 02 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 82 02 0f 00 30 82 02 0a 02 82 02 01 00 86 69 73 7e a3 b5 31 d8 23 e1 6d dd a4 13 d3 54 15 f5 02 eb dc 03 21 b5 7e 5d 1d 52 7c 3f 31 eb 9e 09 6c d1 59 38 5e 67 7e 4b 56 8f 75 90 b2 37 0c 35 5a 64 a5 be 4c 10 2c 24 18 c4 6d 89 8c c1 c5 92 4d 66 02 83 9d f7 e1 21 74 f9 cb 43 02 c1 71 b1 7f ab 4c 38 7d 91 2a c6 ff 89 a9 e8 e4 a1 b9 b2 da 10 85 09 89 9a 38 b7 ce f7 4e e4 9d d1 68 f9 0d 6b 77 0e da 40 1b c4 f7 e6 5f ef fb 1a cd f2 e6 fc 3d 24 a8 5f 95 64 83 0f a3 59 fe 0a 42 d3 6f 50 52 c3 ab c9 85 5a 15 27 3c be a3 1c 00 03 5e 9b ec e2 54 cd 63 03 ad c7 dc 90 b5 ba 71 c1 2b 7b 40 96 35 f8 80 ab 99 12 41 e8 1b 8a 46 df e3 7c 32 45 f4 9b 1c 45 05 65 1c 8c 50 74 a0 09 97 ba 1a 56 75 e0 0e 4a ad 93 6a 9d 75 dd e4 08 35 dd ef 88 2f f3 5d c6 f7 5c fb 0a 3b 06 c8 9f 77 a0 92 25 35 2d d4 80 56 c3 e9 5e 78 24 c8 19 de b4 a6 a2 d6 1b cf df 28 67 15 fb 30 a6 ed 0a 6d 5a 27 fa be 85 3b f6 60 ad 72 33 1a e7 7d c8 9e 2a 63 98 05 b1 43 86 75 b9 3b a4 4c 03 bd 37 74 12 bd da 3e 97 44 dd 84 b6 d2 e4 42 eb a3 66 0c be 8d 74 4a b5 a5 8c 22 59 0d 91 62 66 3a 21 e6 12 b4 27 80 7b ed 88 d9 08 72 32 6e 9a ad 5d 74 55 f8 89 a4 c8 e3 46 ba ce 0b c8 06 dc 45 78 3b 36 45 f7 1a 1f bd de af b7 2d 35 45 2a 81 04 f9 ac 58 09 84 c9 85 c7 be ab 42 00 79 39 95 24 a1 d6 f9 93 67 b1 ec ff 86 bb 82 7c e9 b4 b5 e7 4f 78 52 e6 1c 57 4f 61 55 e9 27 99 38 79 13 1f 42 04 a8 a9 2d 2d 96 db 02 81 6a 47 fe 69 56 27 34 25 3a 4b 49 c0 4a ab 76 c6 b6 69 18 2d 6f ee fe 83 86 e7 a9 cb 22 6d 9f 7a 92 57 63 e8 06 25 39 4a a9 7e 68 04 69 c1 48 9b 40 c1 a6 e3 88 23 c8 d0 ea 0e 55 69 f9 28 4b 42 55 07 f7 1f 02 03 01 00 01 a3 82 01 75 30 82 01 71 30 1f 06 03 55 1d 23 04 18 30 16 80 14 53 79 bf 5a aa 2b 4a cf 54 80 e1 d8 9b c0 9d f2 b2 03 66 cb 30 1d 06 03 55 1d 0e 04 16 04 14 c8 d9 78 68 a2 d9 19 68 d5 3d 72 de 5f 0a 3e dc b5 86 86 a6 30 0e 06 03 55 1d 0f 01 01 ff 04 04 03 02 01 86 30 12 06 03 55 1d 13 01 01 ff 04 08 30 06 01 01 ff 02 01 00 30 1d 06 03 55 1d 25 04 16 30 Data Ascii: 00lU0*H010UUS10UNew Jersey10UJersey City10UThe USERTRUST Network1.0,U%USERTrust RSA Certification Authority020013000000Z300129235959Z0K10UAT10UZeroSSL1*0(U!ZeroSSL RSA Domain Secure Site CA0"0*H0is~1#mT!~]R|?1lY8^g~KVu75ZdL,$mMf!tCqL8}*8Nhkw@_=$_dYBoPRZ'<^Tcq+{@5AF|2EEePtVuJju5/]\;w%5-V^x$(g0mZ';`r3}*cCu;L7t>DBftJ"Ybf:!'{r2n]tUFEx;6E-5E*XBy9$g|OxRWOaU'8yB--jGiV'4%:KIJvi-o"mzWc%9J~hiH@#Ui(KBUu0q0U#0SyZ+JTf0Uxhh=r_>0U0U00U%0

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
Jun 11, 2021 18:08:17.549187899 CEST	20.37.46.234	443	192.168.2.3	49714	CN=20.37.46.234	CN=ZeroSSL RSA Domain Secure Site CA, O=ZeroSSL, C=AT	Thu Jun 10 02:00:00 CEST 2021	Thu Sep 09 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,10-11-13-35-16-23-24-65281,29-23-24,0	1c8f6068d3351ed3651b33bd2625bcdd
Jun 11, 2021 18:08:17.549237013 CEST	20.37.46.234	443	192.168.2.3	49715	CN=20.37.46.234	CN=ZeroSSL RSA Domain Secure Site CA, O=ZeroSSL, C=AT	Thu Jun 10 02:00:00 CEST 2021	Thu Sep 09 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,10-11-13-35-16-23-24-65281,29-23-24,0	1c8f6068d3351ed3651b33bd2625bcdd

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 11, 2021 18:08:21.876784086 CEST	13.32.25.43	443	192.168.2.3	49728	CN=clearbit.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu Apr 22 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sun May 22 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jun 11, 2021 18:08:21.880666018 CEST	13.32.25.43	443	192.168.2.3	49727	CN=clearbit.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu Apr 22 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sun May 22 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jun 11, 2021 18:08:25.292673111 CEST	69.60.184.109	443	192.168.2.3	49730	CN=*.cablelynx.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jul 30 02:00:00 CEST 2019 Mon Nov 06 13:23:33 CET 2017	Thu Jul 29 14:00:00 CEST 2021 Sat Nov 06 13:23:33 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Jun 11, 2021 18:08:25.293534994 CEST	69.60.184.109	443	192.168.2.3	49731	CN=*.cablelynx.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jul 30 02:00:00 CEST 2019 Mon Nov 06 13:23:33 CET 2017	Thu Jul 29 14:00:00 CEST 2021 Sat Nov 06 13:23:33 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=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Jun 11, 2021 18:08:34.232836008 CEST	69.60.184.109	443	192.168.2.3	49735	CN=*.cablelynx.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jul 30 02:00:00 CEST 2019 Mon Nov 06 13:23:33 CET 2017	Thu Jul 29 14:00:00 CEST 2021 Sat Nov 06 13:23:33 CET 2027	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5556 Parent PID: 792

General

Start time:	18:09:04
Start date:	11/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff622950000
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 Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 4420 Parent PID: 5556

General

Start time:	18:09:04
Start date:	11/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5556 CREDAT:17410 /prefetch:2
Imagebase:	0x850000
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 Show Windows behavior

Registry Activities Show Windows behavior

Disassembly

