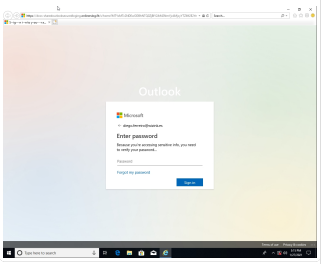
ID: 345082
Cookbook: browseurl.jbs
Time: 17:14:09
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

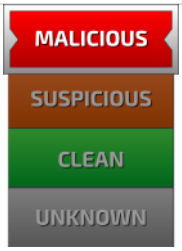
Analysis Report http://huehiufkerfpvkm.craetivehc.com/…

Overview

General Information

Sample URL:	http://huehiufkerfpvkm.craetivehc.com/x/ZGllZ28uZmVycmVpcm9Ad2l6aW5rLmVz
Analysis ID:	345082
Most interesting Screenshot:	

Detection



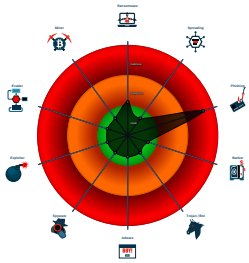
HTMLPhisher

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- Yara detected HtmlPhish_10
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- Invalid T&C link found

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5600 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5824 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5600 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

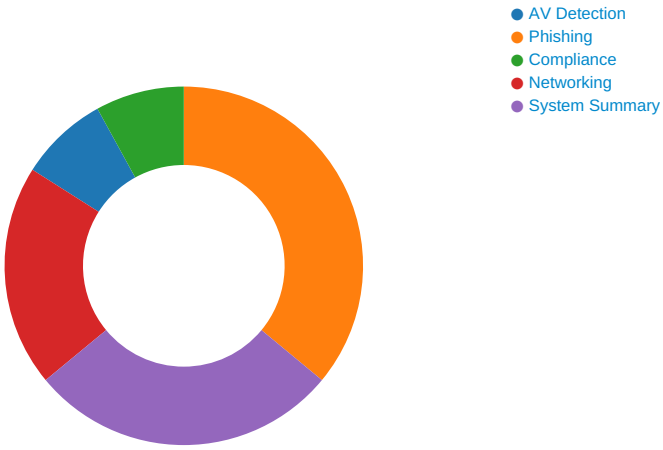
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\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

Antivirus detection for URL or domain

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish_10

Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

Compliance:

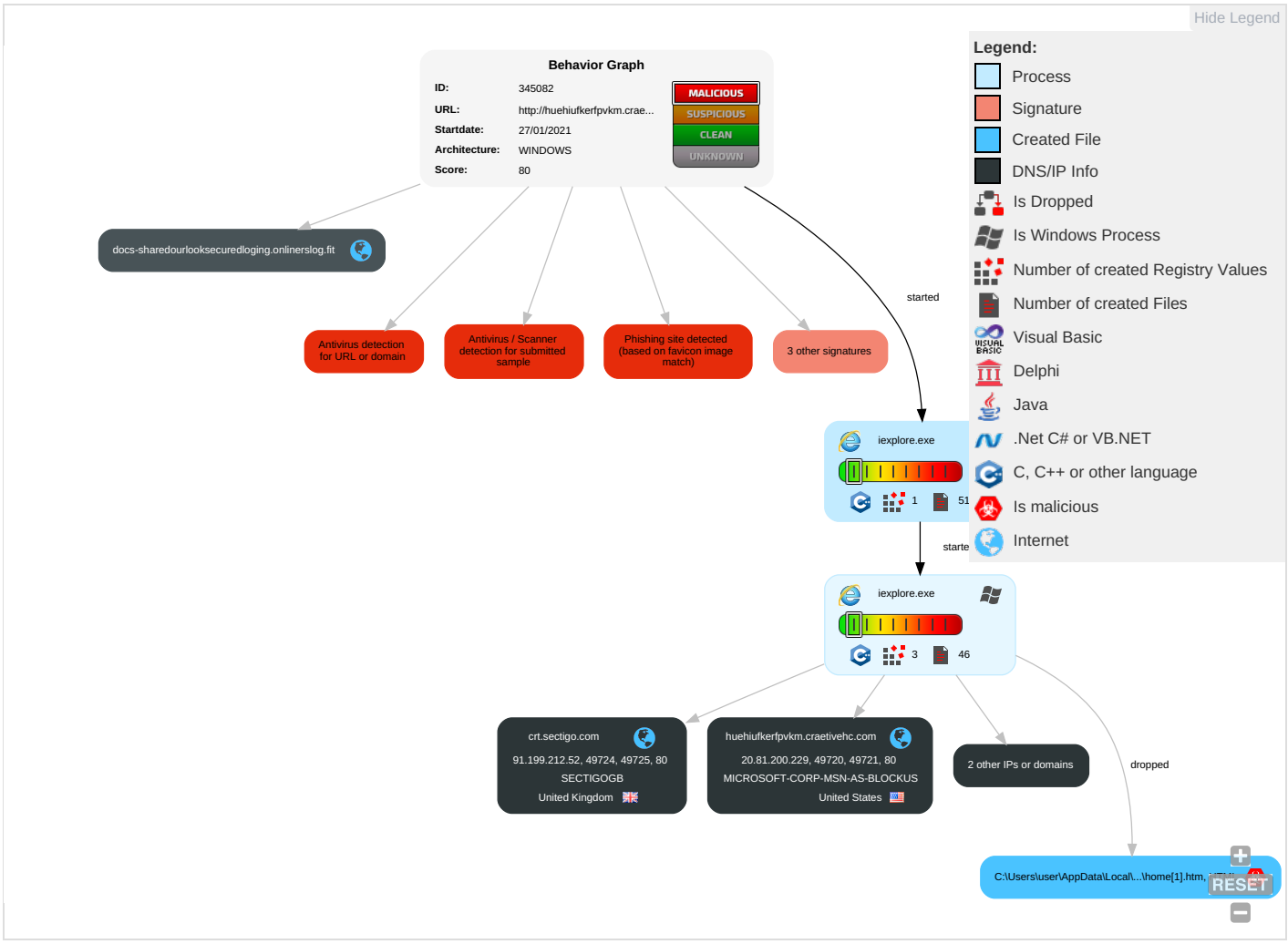
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	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

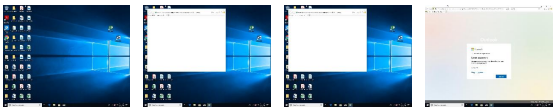
Behavior Graph

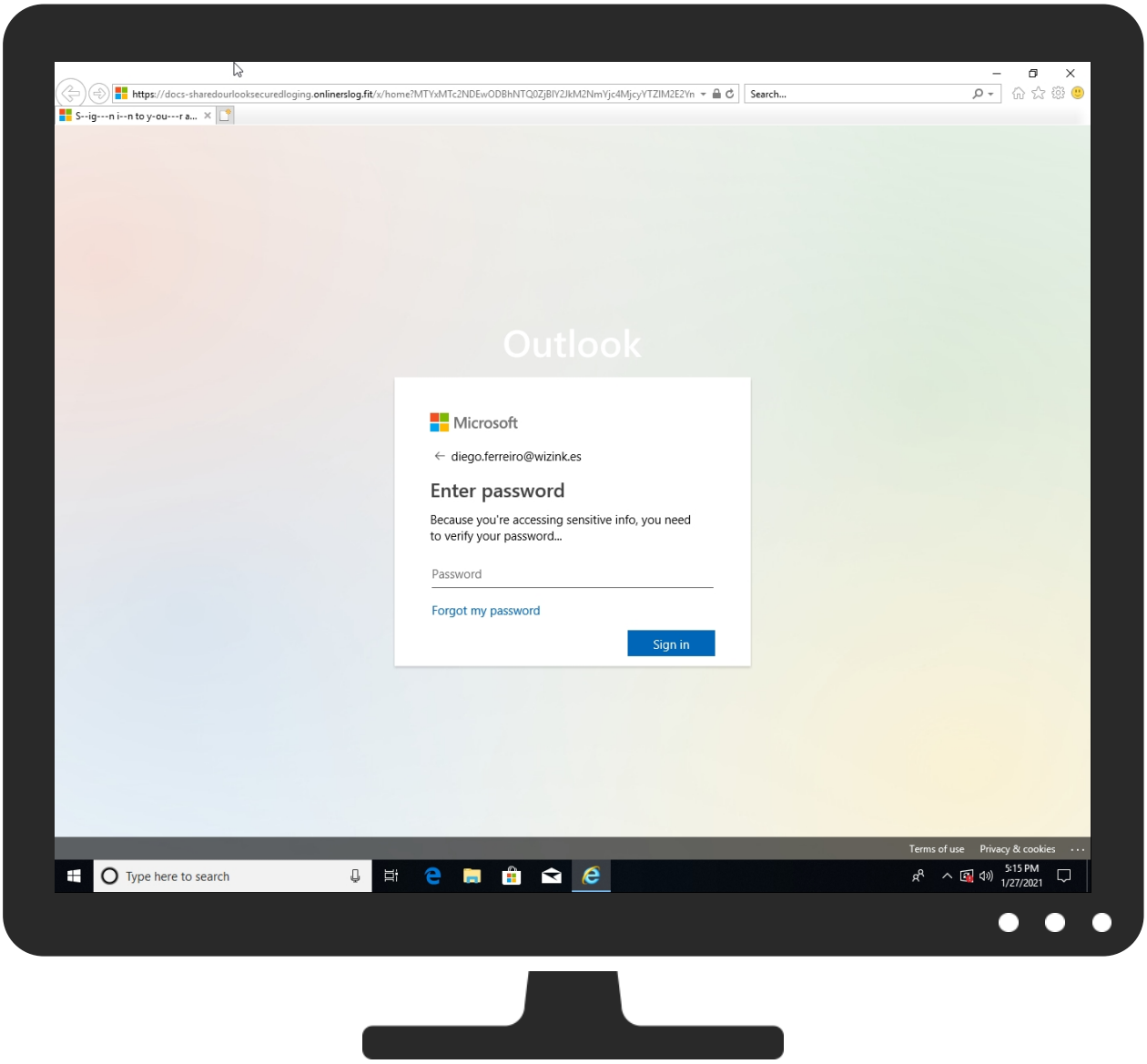


Screenshots

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://huehiufkerfpvkm.craetivehc.com/x/ZGllZ28uZmVycmVpcm9Ad2l6aW5rLmVz	0%	Avira URL Cloud	safe	
http://huehiufkerfpvkm.craetivehc.com/x/ZGllZ28uZmVycmVpcm9Ad2l6aW5rLmVz	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
docs-sharedourlooksecuredloging.onlinerslog.fit	1%	Virustotal		Browse
crt.sectigo.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://docs-sharedourlooksecuredloging.onlinerslog.fit/x/home?MTYxMTc2NDEwODBhNTQ0ZjBlY2JkM2NmYjc4MjcyYTZlM2E2YmYwNjMwNmFhNDM5N2U0NzlhMDZiMDQ2ZGI5Y2RlMTIxMjZlZmZmMThlOGRkNQ==&data=ZGllZ28uZmVycmVpcm9Ad2l6aW5rLmVz&email=diego.ferreiro@wizink.es&MTYxMTc2NDEwOGExZTE4OGY1ZTFlNTA0ZjViN2NkMDRhNzdhODlhMWY1NzRkZDE3OGEwNTI3ZjA2N2E1NGU3OWM0ZDU0YjQ0MjQ1YTZiMjBlYQ==%3D	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://docs-sharedourlooksecuredloging.onlinerslog.fit/x/lib/img/favicon.ico~(	0%	Avira URL Cloud	safe	
http://huehiufkerfpvkm.craetivehc.com/x/ZGllZ28uZmVycmVpcm9Ad2l6aW5rLmVzRoot	0%	Avira URL Cloud	safe	
http://https://docs-sharedourlooksecuredloging.onlinerslog.fit/x/?diego.ferreiro	0%	Avira URL Cloud	safe	
http://https://docs-sharedourlooksecuredloging.onlinerslog.fit/x/home?MTYxMTc2NDEwODBhNTQ0ZjBlY2JkM2NmYjc4M	0%	Avira URL Cloud	safe	
http://https://docs-sharedour.craetivehc.com/x/ZGllZ28uZmVycmVpcm9Ad2l6aW5rLmVzlooksecuredloging.onlinerslo	0%	Avira URL Cloud	safe	
http://zerossl.crt.sectigo.com/ZeroSSLRSADomainSecureSiteCA.crt	0%	Avira URL Cloud	safe	
http://https://docs-sharedourlooksecuredloging.onlinerslog.fit/x/lib/img/favicon.ico	0%	Avira URL Cloud	safe	
http://https://docs-sharedourlooksecuredloging.onlinerslog.fit/x/lib/img/favicon.ico~	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
docs-sharedourlooksecuredloging.onlinerslog.fit	40.84.135.214	true	false	• 1%, Virustotal, Browse	unknown
crt.sectigo.com	91.199.212.52	true	false	• 1%, Virustotal, Browse	unknown
huehiufkerfpvkm.craetivehc.com	20.81.200.229	true	false		unknown
zerossl.crt.sectigo.com	unknown	unknown	false		unknown

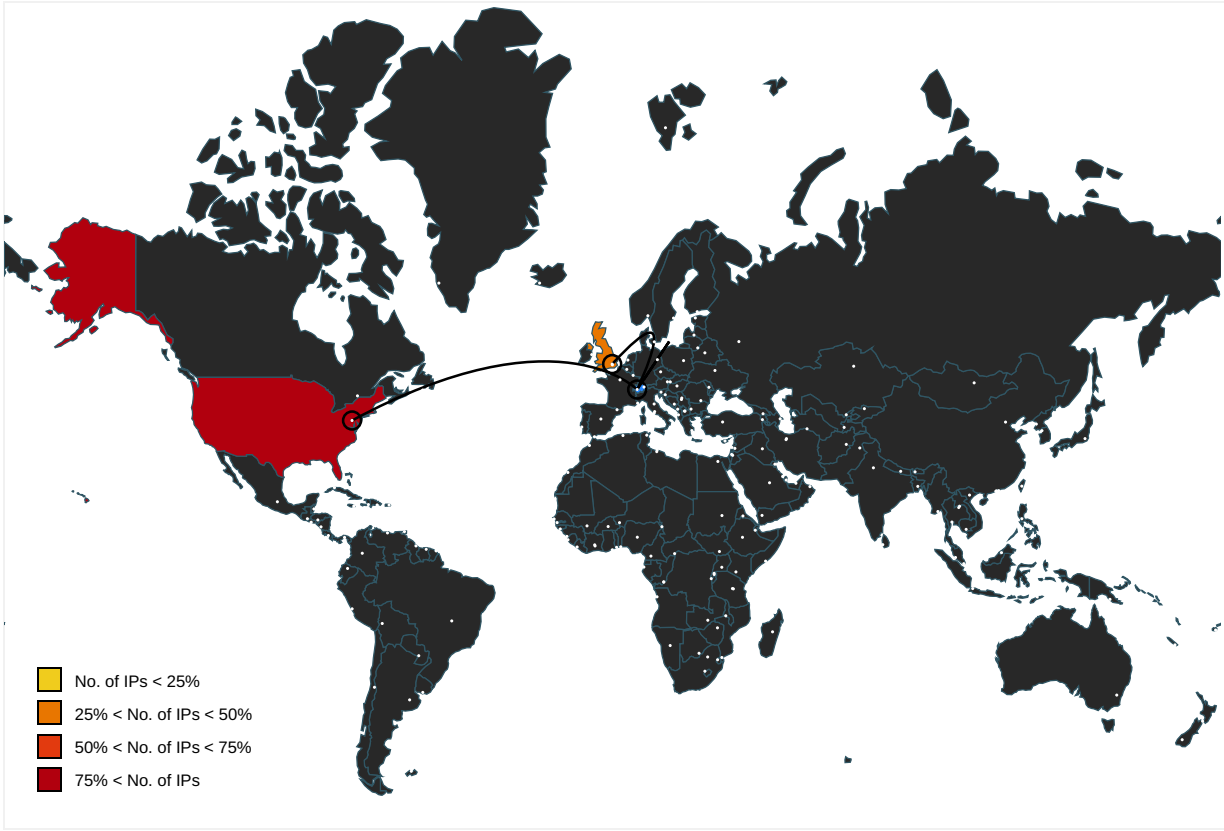
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://docs-sharedourlooksecuredloging.onlinerslog.fit/x/home?MTYxMTc2NDEwODBhNTQ0ZjBlY2JkM2NmYjc4MjcyYTZlM2E2YmYwNjMwNmFhNDM5N2U0NzlhMDZiMDQ2ZGI5Y2RlMTIxMjZlZmZmMThlOGRkNQ==&data=ZGllZ28uZmVycmVpcm9Ad2l6aW5rLmVz&email=diego.ferreiro@wizink.es&MTYxMTc2NDEwOGExZTE4OGY1ZTFlNTA0ZjViN2NkMDRhNzdhODlhMWY1NzRkZDE3OGEwNTI3ZjA2N2E1NGU3OWM0ZDU0YjQ0MjQ1YTZiMjBlYQ==%3D	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://huehiufkerfpvkm.craetivehc.com/x/ZGllZ28uZmVycmVpcm9Ad2l6aW5rLmVz	true		unknown
http://zerossl.crt.sectigo.com/ZeroSSLRSADomainSecureSiteCA.crt	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://docs-sharedourlooksecuredloging.onlinerslog.fit/x/lib/img/favicon.ico~(	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://huehiufkerfpvkm.craetivehc.com/x/ZGllZ28uZmVycmVpcm9Ad2l6aW5rLmVzRoot	{3F72F0F0-6106-11EB-90E5-ECF4BB570DC9}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://docs-sharedourlooksecuredloging.onlinerslog.fit/x/?diego.ferreiro	ZGllZ28uZmVycmVpcm9Ad2l6aW5rLmVz[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://docs-sharedourlooksecuredloging.onlinerslog.fit/x/home?MTYxMTc2NDEwODBhNTQ0ZjBlY2JkM2NmYjc4M	~DF356D71385CE4B18E.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://docs-sharedour.craetivehc.com/x/ZGllZ28uZmVycmVpcm9Ad2l6aW5rLmVzlooksecuredloging.onlinerslo	{3F72F0F0-6106-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://docs-sharedourlooksecuredloging.onlinerslog.fit/x/lib/img/favicon.ico	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://docs-sharedourlooksecuredloging.onlinerslog.fit/x/lib/img/favicon.ico~	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
20.81.200.229	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
40.84.135.214	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
91.199.212.52	unknown	United Kingdom		48447	SECTIGOGB	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345082
Start date:	27.01.2021
Start time:	17:14:09
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://huehiufkerfpvkm.craetivehc.com/x/ZGllZ28uZmVycmVpcm9Ad2l6aW5rLmVz
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:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal80.phis.win@3/18@4/3
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 104.43.193.48, 104.108.39.131, 23.210.248.85, 51.104.139.180, 95.101.22.125, 95.101.22.134, 152.199.19.161 • Excluded domains from analysis (whitelisted): fs.microsoft.com, arc.msn.com.nsatc.net, ie9comview.vo.msecnd.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\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):	3.095107598593844
Encrypted:	false
SSDEEP:	6:kK4EY4qMUjKFgJE5Y7EyUWOJ9jnsKtfY4qMUjKFgJE5Y7EyUWOJ9jn/:wEY4qMUE0WYtBoxnxY4qMUE0WYtBoxn/
MD5:	EAA31D5E30E2F185529653528A02185C
SHA1:	8D9FCF5C4F5C4D06F3DE4850FBD775CAD61980D0
SHA-256:	AA25C54684A02BC189C8EC2480B63B5229F3F2C54737F0904F940EFE367074AD
SHA-512:	A1EDC6A8B75F7E38416ECD5BE584D2504CD79A483EC574238E92CD05B47B67446793A85F43B34712C96BC3DF80BC1AB1FE097BEFA7E0EB62BE625E7348E0A5C3
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..... .....H2.....(..... .....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\Recovery\High\Active\RecoveryStore.{3F72F0EE-6106-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8499809915792826
Encrypted:	false
SSDEEP:	96:rlZ5Zt2Xu9WXItXwbfXEovKMX5XqXc9QXgxfXeom6X:rlZ5Zt2+9W4twfURME/+fu8X
MD5:	8005B39A115CE6162BE3AA44B5144D0C
SHA1:	7B190B9F53C890D430AF829BC7C0F995A7AAF40F
SHA-256:	F2332F16BC3A5974D47D47ACF91E68AEFBF397907A24D0F59F847BAAFD6611EF
SHA-512:	40786C9123BC7FBC914403610041E2582F08BE523F0D42FD5AA460EEF544091600266E59A40039074D3D45B1F8EBE086DB4394CA211FD9220E61B96590A69E3B
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\{3F72F0F0-6106-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33368
Entropy (8bit):	2.266230339485313
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{3F72F0F0-6106-11EB-90E5-ECF4BB570DC9}.dat	
SSDEEP:	192:ruZBQ96DksFjx2EkWQMzYbPO80eC0ZD0s0W0f0ufL:r6WoIshgwlzumd8ZYt7MuT
MD5:	F13AEC1B649C8A2678CAD4FD7B958A13
SHA1:	626099648B60ABCE10856264D729863EEE033AA8
SHA-256:	6B03DEE17A2997D23BF047F7CE0E721DC2B63E53B9DAFFF9A826A478C75B1BA9
SHA-512:	47DF8094D772826D6BB5EC7E1BBAA0360A1F39A8BC6C54B3577B8F334FD93EA09F98F0B4AD9729291139D883EDD428FF3F758B3C0C20910A15A1078CCDBA7A9 C
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\{4994EEBB-6106-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5640311352383127
Encrypted:	false
SSDEEP:	48:IwNGcprcGwpaVG4pQxGrapbScrGQpKOG7HpR+sTGIpG:rTZUQH6BBScFAJT+4A
MD5:	CB05B5A920A18CC364206FDB2A88B7FA
SHA1:	1DF2FC99155828967D42D2D206478DB18C576DFB
SHA-256:	41246BA932A4C681B4BDE812027B040283904C5E1EC5C9EB51028ED2890AB248
SHA-512:	C9B37AEB3DB7EFE08A25E6552D346976F865E917A222441BE0AC9D4F27145ABEA21B827FCBC38EC443C20D7521A0C8612226BA7F3697D7025DAE60F473D0CF3 D
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y... ....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\dikxvqf\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	18356
Entropy (8bit):	3.1144171316444202
Encrypted:	false
SSDEEP:	48:mP0efaE/EqP0efaE/bqP0efaE/jqP0efaE/tgyyyyyyyyyyyyyIqP0efaE/D/qPR:00M0z0z0w0b0jQQQQQZ
MD5:	9E43E23A22D2584F44841947BB9617EA
SHA1:	B4C939866E13C0B9F1FEEAC81283F32CAC695620
SHA-256:	91D3C714D124D131663AB4105276E05C8F2E7639EF38B50084FB5212D493F44E
SHA-512:	2EFD1BEE29133230C0A4E771BBC542CA9D55117AE2102348F2A7806B26DCDE38B23B7F82247BC711DFC6E0468223E45FB6EF548D05995FE3A392F1ACA21847B
Malicious:	false
Reputation:	low
Preview:	M.h.t.t.p.s.:././.d.o.c.s.-.s.h.a.r.e.d.o.u.r.l.o.o.k.s.e.c.u.r.e.d.l.o.g.i.n.g...o.n.l.i.n.e.r.s.l.o.g...f.i.t./.x./.l.i.b./.i.m.g./.f.a.v.i.c.o.n...i.c.o.~(................h(......(....................(................ ...."P..."""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333 333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333 333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""" """""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...333333333333333 33333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\background[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=4, xresolution=62, yresolution=70, resolutionunit=2], progressive, precision 8, 1920x1080, frames 3
Category:	downloaded
Size (bytes):	31419
Entropy (8bit):	7.838593850267985
Encrypted:	false
SSDEEP:	768:B2CG6sPLHj1DDtLEHZwbz0yDEr+q5jc0T7KEE:4CG6sTDFRLKZwbzpDEr+Zc7e
MD5:	B204756661AE1F820ACDBF507B2C0FE7
SHA1:	8BCC62CD820991FE0C4D35C2E397E9D2E225D4A0
SHA-256:	A33593E9043EFEFBAF94D9CA220C885CE1C42DD2A7707F30ED072D7D71587DA5
SHA-512:	F115CD7216716F759575B0411028CFA56049150F54D2692CF8998E47D82959BA1521CB9462DF6E5496C51B08ED736FFC0CF4BB70C0328099143293CDDB4B570E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\background[1].jpg	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://docs-sharedourlooksecuredloging.onlinerslog.fit/x/lib/img/background.jpg
Preview:	.....JFIF.....`.`.....VExif..MM.*.....>.....F.(.....`.....`.....! !,.;.....! !,,;.....8. ..."..... .....&`...n.... .Z...&.P....UZ. ....%`....d.j...[@.....@.....C9kD...4..k@.Z36-jP..Y...2...f....4.....b...*....uA..t..b.....3 .T....n....f... .+"KR..A.FC.`.d&..f. !t...@]P]P...b...g ....d.t...@.-.&..)."..D.i.J.....2X@.H.HR.....T.`...0.D..0.....3.....@.....hH....sL.. ...r[I.Am.U.]Pn.@..0.kL.&`.2.n.L....h.5..@bS[U.$-f@.1.ee5....".$...E.....k L..w 9.....`h.....m..e..f.....$S9-&a...`.U..R....7B..... ....P.:.....V..Z..P.U.# .s...$.&...&.....Ahk@.....9].....V..B,u%R...h.7r.w6....,.a5-.....@."f..J..]...{.uCt..b...rD.4$l@.....i2]..... ..%...&..a0.....h....7rkE.LCy.9...$.*..u@.oi..]Vd7B.T...3fE....."..].H.M..uQ.QjK.sg&....%.$...@n....5)M.eu@.U(....H..*`3.&a2hFi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\logo2[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://docs-sharedourlooksecuredloging.onlinerslog.fit/x/lib/img/logo2.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38 .119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392, 1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47. 081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0, 0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.61 1,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.9 52,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\ZGllZ28uZmVycmVpcm9Ad2l6aW5rLmVz[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	149
Entropy (8bit):	4.69713648664703
Encrypted:	false
SSDEEP:	3:gnkAqRAdu6/GY7voOkADFoHDtL/QUJYC5LAeKCLr0dTgYBXILn:7AqJm7+mmHhZJBLzKIAgCYL
MD5:	CA1AE28154FE294016416ECCEB7C618D
SHA1:	90DAA9B614BDE0D09C77AD6F395EE106516B9540
SHA-256:	FAB2876CD18840FB88240F181D4AE1E03944EC25ED35CC7072797305C3113CB0
SHA-512:	C35358C2D01DE5950BB8B8B166CBB5420C38E99EE137E02FE900E083B143FEF16B6C93D14E76731AD06F658D084148FC86EB3A0B57C876D729E4713DBB7E870
Malicious:	false
Reputation:	low
IE Cache URL:	http://huehiufkerfpvkm.craetivehc.com/x/ZGllZ28uZmVycmVpcm9Ad2l6aW5rLmVz
Preview:	<script type="text/javascript">window.location.href = "https://docs-sharedourlooksecuredloging.onlinerslog.fit/x/?diego.ferreiro@wizink.es"</script>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 6 icons, 128x128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsQZp:nfgyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://docs-sharedourlooksecuredloging.onlinerslog.fit/x/lib/img/favicon.ico

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\favicon[1].ico

Preview:	.............h(..f...HH..........(..00......h....6.. ....=..............@.........(....A..(..................(..................................."P......................................."""""""""""""""""""""""""""""""" ...3 3333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""" """""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333 33333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""""" """""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333 333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333""""""""""""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\arrow[1].svg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	513
Entropy (8bit):	4.720499940334011
Encrypted:	false
SSDEEP:	12:t4BdU/uRqv6DLfBHKFWJCDLfBSU1pRXIFl+MJ4bADc:t4TU/uRff0EcfIU1XXU+t2c
MD5:	A9CC2824EF3517B6C4160DCF8FF7D410
SHA1:	8DB9AEBAD84CA6E4225BFDD2458FF3821CC4F064
SHA-256:	34F9DB946E89F031A80DFCA7B16B2B686469C9886441261AE70A44DA1DFA2D58
SHA-512:	AA3DDAB0A1CFF9533F9A668ABA4FB5E3D75ED9F8AFF8A1CAA4C29F9126D85FF4529E82712C0119D2E81035D1CE1CC491FF9473384D211317D4D00E0E234AD9 F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://docs-sharedourlooksecuredloging.onlinerslog.fit/x/lib/img/arrow.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="24" height="24" viewBox="0 0 24 24"><title>assets</title><path d="M18,11.578v.844H7.617l3.921,3.928-.594.594L6,12 l4.944-4.944.594.594L7.617,11.578Z" fill="#404040"/><path d="M10.944,7.056l.594.594L7.617,11.578H18v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944m0-.141-.071.07L5.929,11.929,5.858,12l.071.071,4.944,4.944.071.07.071-.07.594-.595.071-.07-.071-.071L7.858,12.522H18.1V11.478H7.858l3.751-3.757.071-.071-.071-.07-.594-.595-.071-.07Z" fill="#404040"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\white_ellipsis[1].svg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	915
Entropy (8bit):	3.877322891561989
Encrypted:	false
SSDEEP:	24:t4CvnAVRf83f1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUV0Uv6f1QqCWbVHTVeUV0W:fnL1QqC4GuiHFXS1QqCWRHQ3V1QqCWRV
MD5:	5AC590EE72BFE06A7CECFD75B588AD73
SHA1:	DDA2CB89A241BC424746D8CF2A22A35535094611
SHA-256:	6075736EA9C281D69C4A3D78FF97BB61B9416A5809919BABE5A0C5596F99AAEA
SHA-512:	B9135D934B9EA50B51BB0316E383B114C8F24DFE75FEF11DCBD1C96170EA59202F6BAFE11AAF534CC2F4ED334A8EA4DBE96AF2504130896D6203BFD2DA6913 F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://docs-sharedourlooksecuredloging.onlinerslog.fit/x/lib/img/white_ellipsis.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path fill="#ffffff" d="M1.143,6.857a1.107,1.107,0,0,1,. 446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,.7,9.054a1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893A1.164,1.164,0,0,1,.7,6.946a1.107,1.107,0,0,1,.446-.089M8,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.1 61,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107 ,0,0,1,8,6.857m6.857,0a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164, 1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,14.857,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\home[1].htm

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	4896
Entropy (8bit):	3.9126979104150483
Encrypted:	false
SSDEEP:	48:tcFIqr5Wxn1PWWmvw0vqcRvZ82gBIZflx3v:8Iq1K9WNBnvZGIZPv
MD5:	3B84D0C9225D24FC7E5152CB6A2D598F
SHA1:	7A5333C492C1BC12C5610C22D619EF9D04E70247
SHA-256:	45364A073B31276BC6EAD8526712AD2B6028094877BF248076FD507432CBAAD8
SHA-512:	D1AB93213C0412B9E0CECC784251931130306549BDE99463A27B0DC28A462F72F1EBDA3717460ED54A9A255F3EC7A01D345360192A9D6434F2330ABE515AB9FF
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\home[1].htm, Author: Joe Security
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\home[1].htm	
Preview:	<!DOCTYPE html>..<html dir="ltr" lang="en">..<title>S..ig...n i..n to y.ou...r ac...cou..nt</title>..<link href="lib/img/favicon.ico" rel="shortcut icon">..<link href="lib/css/login.css" rel="stylesheet">>.. .. .. <form method="post" action="" name="login_form">.. .. .. ..<img src="lib/img/logo3.png" class="background-logo">.. .. ..<img src="lib/img/logo2.svg" class="logo">.. .. ..<img src="lib/img/arrow.svg">...... diego.ferreiro@wizink.es .. ..</di

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\login[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	101788
Entropy (8bit):	5.304944776832708
Encrypted:	false
SSDEEP:	1536:QpHDglbuhw+ExmazA/PWrF7qvEAFiQcpmNtuhPyJRD:l74wyJZ
MD5:	4DB4A299AE7E73B3CB53351867416D0C
SHA1:	36C0DFF7A6742EAD3229E476F05C559069C3080F
SHA-256:	10C50B88EBF99FDF813A4CCE86BA218A6E2EA3D266146520529F1E1BDDC5EBD3
SHA-512:	8EB086FC241C314DDD4B15AC6F34DBD61B838E2D7C2B535A02AF2A83A92294AB1C79EB122EFCA8FF648346F4515B35EDEEB13DC5E79EBC2C7E9ACCC4AC5BAA76
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://docs-sharedourlooksecuredloging.onlinerslog.fit/x/lib/css/login.css
Preview:	/*! Copyright (C) Microsoft Corporation. All rights reserved. */*!.---------- START OF THIRD PARTY NOTICE ----------..This file based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise...//----------.twbs-bootstrap-sass (3.3.0).//----------..The MIT License (MIT)..Copyright (c) 2013 Twitter, Inc..Permission is hereby granted, free of charge, to any person

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\logo3[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 342 x 72, 4-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1750
Entropy (8bit):	7.784821733371315
Encrypted:	false
SSDEEP:	24:W6Yai7i2Tz46sC7PbpHZMYYsOWFzyKgXW0n9/ND1LCgz7AXtew1pcv8m5PRlQXt+:9KtTzx/HxRF+KKWE/B1LCgYXtIZRlN
MD5:	533E293F0C8947ADA653B47C00E394E2
SHA1:	0F507BB89C42F937A290D0EEDA3F2E0DBFCAD5C1
SHA-256:	B5D587F6C48A9B22BBE97150249E0C0655AC1780BD273431480A22F8A5BFEF6C
SHA-512:	B91127D6C27E270F7AAB0A83054451FFF4719C587A425F36EC32F4E532CF4E4D74505AAC71ED3629769552924BC9A9C8CB7F73667B0D20EA5AAED587BCD3E17
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://docs-sharedourlooksecuredloging.onlinerslog.fit/x/lib/img/logo3.png
Preview:	.PNG.....IHDR...V...H....._*.....gAMA.....a.....sRGB.....0PLTEGpL.....D>.....tRNS.w.D...3f..".U...1;...)IDATh..ZMh\U...t&...L#..:I(.P..7..T$V....1h....Eq!..Q.....q.....&Bq.Up.".B..$.L..Os...}..s...%3.w.....=..s...a....T.9.i.....'...\.7X...~.....c.....3.`.6.Z.T.....m..U.YM*.....K-..Y..g...<..-.z...Bs.....uZ;.F.w...Y..m.....m.....jMYI..RkzQ.{]..V...i..i.R.V...e..yj....Mk..[g.y#h..,.u.].K.f..d.....b.u..L.a..Kk...5r....Rk...v.\../..Ekz.....i..,.K..?F.....).<..x...=o.k..}'g.0.o...n.....K.L..l..B...5.....4..`.CD+...-1...E.((.=k.....}.H.dqe.Q..b.%.C.\.e..=...m.\k.".4_.....Y5.S.....U....j.ZV.*wY;..^.X.....&.1.!.*..;m,..?..`.<t.Z....3@...../...j..rC>x>.e.,.=...F.....p..U...J...5d....>.~d._\.....o.....j...\.z8.8..a...<.MI8.]...3.V.Z.G....V.S..ta.c.m..Z."k.&y....a....p..Z.h..q..a.#.....s>4O}.F.&9....R.$....\....>..0....F.."....8f.....i-X....".aX.1....j..#k.c.U.9).ta.#K..!..z..zXD...&8.

C:\Users\user\AppData\Local\Temp\~DF12B82F2018A6403B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.3245043509657957
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAAvOAM:kBqoxxJhHWSVSEabAvOA
MD5:	DF2958624447487DF004C835F737F326
SHA1:	C404AA80B34E07D70249BA53B89B07DEB6559857
SHA-256:	E43056E46F864A0D969E2EB30C8D2FC716E2EA8C43059863EDA47403C0958ADB
SHA-512:	20AF848CF40C74DC74D5095A2180F02F0E5866B199F7F20594A015D4BF4BAEA82992E9B0BBF2EE984C89F1ACEBC8F57C97F90D49DA77C6B92379EC1E1B2C72A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DF12B82F2018A6403B.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF356D71385CE4B18E.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	43818
Entropy (8bit):	0.9608238901188655
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+2wqDwfKM80Y0ZD0s0W0f0u:kBqoxKAuqR+2wqDwfKMdBZYt7Mu
MD5:	5A52D0F75F0520AF194E4FC9564DF10E
SHA1:	EF4B17897F8C89C4F566F06F358120EB6085375F
SHA-256:	347EE3B7C6AC98ADE4EBD763C295166CBAB4DD90D0A7C329C8621D61914D089F
SHA-512:	D88C0B69D95F3593DB6BC223170528427291BB35A981D83F8E919ADD6C6A394563BAC6BB7E70C1708FCA5A47BF6AD1E209D6F746D5584B0D800A8997C76576D
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFD27693C6AAB55A24.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4791783023883562
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loUT9loUT9lWUkMp6apOR9ORP7O7Q:kBqoIzlXA
MD5:	B563C982C2EC8AABB037DF49DD26BA1F
SHA1:	91AF55CF61820213E9D781EF947B4DCBEA28DBB1
SHA-256:	8F12BBCD1E5D0C94F5C3BE723DBAAA5B3FB7577E000463E9A8C7799693536819
SHA-512:	824D55BE603680B57A50FB1EAB293F897E39F10F2550FA8CE6D76C53F462A2785422016666EE159A2B77AC910A152B2446F8AE46FB6DFDB9EDA9908735FCF91E
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: 71

- 53 (DNS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 17:15:05.565825939 CET	49721	80	192.168.2.5	20.81.200.229
Jan 27, 2021 17:15:05.565910101 CET	49720	80	192.168.2.5	20.81.200.229
Jan 27, 2021 17:15:05.694519997 CET	80	49721	20.81.200.229	192.168.2.5
Jan 27, 2021 17:15:05.694710016 CET	49721	80	192.168.2.5	20.81.200.229
Jan 27, 2021 17:15:05.694781065 CET	80	49720	20.81.200.229	192.168.2.5
Jan 27, 2021 17:15:05.694871902 CET	49720	80	192.168.2.5	20.81.200.229
Jan 27, 2021 17:15:05.695318937 CET	49721	80	192.168.2.5	20.81.200.229
Jan 27, 2021 17:15:05.889887094 CET	80	49721	20.81.200.229	192.168.2.5
Jan 27, 2021 17:15:06.061757088 CET	80	49721	20.81.200.229	192.168.2.5
Jan 27, 2021 17:15:06.061872959 CET	49721	80	192.168.2.5	20.81.200.229
Jan 27, 2021 17:15:06.591379881 CET	49723	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:06.594357014 CET	49722	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:06.745685101 CET	443	49723	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:06.745804071 CET	49723	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:06.751168013 CET	443	49722	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:06.751302004 CET	49722	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:06.754837990 CET	49723	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:06.755206108 CET	49722	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:06.910450935 CET	443	49723	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:06.910489082 CET	443	49723	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:06.910557032 CET	49723	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:06.910593987 CET	49723	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:06.912173986 CET	443	49722	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:06.912203074 CET	443	49722	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:06.912344933 CET	49722	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:07.652102947 CET	49724	80	192.168.2.5	91.199.212.52
Jan 27, 2021 17:15:07.653048992 CET	49725	80	192.168.2.5	91.199.212.52
Jan 27, 2021 17:15:07.716795921 CET	80	49724	91.199.212.52	192.168.2.5
Jan 27, 2021 17:15:07.716835976 CET	80	49725	91.199.212.52	192.168.2.5
Jan 27, 2021 17:15:07.716984987 CET	49724	80	192.168.2.5	91.199.212.52
Jan 27, 2021 17:15:07.717055082 CET	49725	80	192.168.2.5	91.199.212.52
Jan 27, 2021 17:15:07.762238026 CET	49725	80	192.168.2.5	91.199.212.52
Jan 27, 2021 17:15:07.763355017 CET	49724	80	192.168.2.5	91.199.212.52
Jan 27, 2021 17:15:07.826227903 CET	80	49725	91.199.212.52	192.168.2.5
Jan 27, 2021 17:15:07.826288939 CET	80	49725	91.199.212.52	192.168.2.5
Jan 27, 2021 17:15:07.826327085 CET	80	49725	91.199.212.52	192.168.2.5
Jan 27, 2021 17:15:07.826467991 CET	49725	80	192.168.2.5	91.199.212.52
Jan 27, 2021 17:15:07.827028990 CET	80	49724	91.199.212.52	192.168.2.5
Jan 27, 2021 17:15:07.827099085 CET	80	49724	91.199.212.52	192.168.2.5
Jan 27, 2021 17:15:07.827132940 CET	80	49724	91.199.212.52	192.168.2.5
Jan 27, 2021 17:15:07.827265978 CET	49724	80	192.168.2.5	91.199.212.52
Jan 27, 2021 17:15:07.856863022 CET	49723	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:07.856904030 CET	49722	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:07.857686043 CET	49722	443	192.168.2.5	40.84.135.214

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 17:15:08.013705969 CET	443	49723	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:08.013797045 CET	49723	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:08.014425039 CET	443	49722	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:08.014508009 CET	49722	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:08.066127062 CET	443	49722	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:08.422846079 CET	443	49722	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:08.423005104 CET	49722	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:08.425647020 CET	49722	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:08.637414932 CET	443	49722	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:10.570102930 CET	80	49724	91.199.212.52	192.168.2.5
Jan 27, 2021 17:15:10.570126057 CET	80	49725	91.199.212.52	192.168.2.5
Jan 27, 2021 17:15:10.570168972 CET	49724	80	192.168.2.5	91.199.212.52
Jan 27, 2021 17:15:10.570195913 CET	49725	80	192.168.2.5	91.199.212.52
Jan 27, 2021 17:15:10.570285082 CET	49724	80	192.168.2.5	91.199.212.52
Jan 27, 2021 17:15:10.570350885 CET	49725	80	192.168.2.5	91.199.212.52
Jan 27, 2021 17:15:10.634191990 CET	80	49724	91.199.212.52	192.168.2.5
Jan 27, 2021 17:15:10.634243011 CET	80	49725	91.199.212.52	192.168.2.5
Jan 27, 2021 17:15:11.558188915 CET	80	49721	20.81.200.229	192.168.2.5
Jan 27, 2021 17:15:11.558337927 CET	49721	80	192.168.2.5	20.81.200.229
Jan 27, 2021 17:15:13.037166119 CET	443	49722	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:13.037369967 CET	49722	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:13.042767048 CET	49722	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:13.262533903 CET	443	49722	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:13.307244062 CET	443	49722	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:13.307270050 CET	443	49722	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:13.307287931 CET	443	49722	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:13.307302952 CET	443	49722	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:13.307316065 CET	49722	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:13.307358980 CET	49722	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:13.326982021 CET	49722	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:13.327754021 CET	49723	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:13.329811096 CET	49726	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:13.330950975 CET	49727	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:13.331463099 CET	49728	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:13.484667063 CET	443	49722	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:13.484693050 CET	443	49722	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:13.484709978 CET	443	49722	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:13.484725952 CET	443	49722	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:13.484730005 CET	49722	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:13.484739065 CET	443	49722	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:13.484759092 CET	443	49722	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:13.484767914 CET	49722	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:13.484781027 CET	443	49722	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:13.484793901 CET	443	49722	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:13.484810114 CET	443	49722	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:13.484812975 CET	49722	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:13.484827042 CET	443	49722	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:13.484839916 CET	443	49726	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:13.484841108 CET	49722	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:13.484872103 CET	49722	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:13.484916925 CET	49726	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:13.485816956 CET	443	49728	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:13.485935926 CET	49728	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:13.486330032 CET	49726	443	192.168.2.5	40.84.135.214
Jan 27, 2021 17:15:13.486387014 CET	443	49727	40.84.135.214	192.168.2.5
Jan 27, 2021 17:15:13.486458063 CET	49727	443	192.168.2.5	40.84.135.214

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 17:14:59.216414928 CET	65296	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:14:59.267267942 CET	53	65296	8.8.8.8	192.168.2.5
Jan 27, 2021 17:15:00.166466951 CET	63183	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:15:00.214437962 CET	53	63183	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 17:15:01.147109985 CET	60151	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:15:01.195234060 CET	53	60151	8.8.8.8	192.168.2.5
Jan 27, 2021 17:15:03.999756098 CET	56969	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:15:04.061264038 CET	53	56969	8.8.8.8	192.168.2.5
Jan 27, 2021 17:15:05.485532045 CET	55161	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:15:05.554894924 CET	53	55161	8.8.8.8	192.168.2.5
Jan 27, 2021 17:15:06.528197050 CET	54757	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:15:06.588871956 CET	53	54757	8.8.8.8	192.168.2.5
Jan 27, 2021 17:15:07.567178965 CET	49992	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:15:07.649831057 CET	53	49992	8.8.8.8	192.168.2.5
Jan 27, 2021 17:15:19.136082888 CET	60075	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:15:19.200200081 CET	53	60075	8.8.8.8	192.168.2.5
Jan 27, 2021 17:15:22.034053087 CET	55016	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:15:22.112302065 CET	53	55016	8.8.8.8	192.168.2.5
Jan 27, 2021 17:15:24.467451096 CET	64345	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:15:24.515644073 CET	53	64345	8.8.8.8	192.168.2.5
Jan 27, 2021 17:15:31.914210081 CET	57128	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:15:31.974792957 CET	53	57128	8.8.8.8	192.168.2.5
Jan 27, 2021 17:15:33.994510889 CET	54791	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:15:34.050858974 CET	53	54791	8.8.8.8	192.168.2.5
Jan 27, 2021 17:15:35.009541035 CET	54791	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:15:35.065922022 CET	53	54791	8.8.8.8	192.168.2.5
Jan 27, 2021 17:15:35.066243887 CET	50463	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:15:35.117003918 CET	53	50463	8.8.8.8	192.168.2.5
Jan 27, 2021 17:15:36.008594990 CET	54791	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:15:36.069551945 CET	53	54791	8.8.8.8	192.168.2.5
Jan 27, 2021 17:15:36.071707010 CET	50463	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:15:36.131751060 CET	53	50463	8.8.8.8	192.168.2.5
Jan 27, 2021 17:15:37.071106911 CET	50463	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:15:37.132862091 CET	53	50463	8.8.8.8	192.168.2.5
Jan 27, 2021 17:15:38.027137041 CET	54791	53	192.168.2.5	8.8.8.8
Jan 27, 2021 17:15:38.085154057 CET	53	54791	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 17:15:05.485532045 CET	192.168.2.5	8.8.8.8	0x1159	Standard query (0)	huehiufker fpvkm.crae tivehc.com	A (IP address)	IN (0x0001)
Jan 27, 2021 17:15:06.528197050 CET	192.168.2.5	8.8.8.8	0xfce3	Standard query (0)	docs-share dourlookse curedlogin g.onlinerslog.fit	A (IP address)	IN (0x0001)
Jan 27, 2021 17:15:07.567178965 CET	192.168.2.5	8.8.8.8	0x5adb	Standard query (0)	zerossl.cr t.sectigo.com	A (IP address)	IN (0x0001)
Jan 27, 2021 17:15:22.034053087 CET	192.168.2.5	8.8.8.8	0x2829	Standard query (0)	docs-share dourlookse curedlogin g.onlinerslog.fit	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 17:15:05.554894924 CET	8.8.8.8	192.168.2.5	0x1159	No error (0)	huehiufker fpvkm.crae tivehc.com		20.81.200.229	A (IP address)	IN (0x0001)
Jan 27, 2021 17:15:06.588871956 CET	8.8.8.8	192.168.2.5	0xfce3	No error (0)	docs-share dourlookse curedlogin g.onlinerslog.fit		40.84.135.214	A (IP address)	IN (0x0001)
Jan 27, 2021 17:15:07.649831057 CET	8.8.8.8	192.168.2.5	0x5adb	No error (0)	zerossl.cr t.sectigo.com	crt.sectigo.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 17:15:07.649831057 CET	8.8.8.8	192.168.2.5	0x5adb	No error (0)	crt.sectigo.com		91.199.212.52	A (IP address)	IN (0x0001)
Jan 27, 2021 17:15:22.112302065 CET	8.8.8.8	192.168.2.5	0x2829	No error (0)	docs-share dourlookse curedlogin g.onlinerslog.fit		40.84.135.214	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- huehiufkerfpvkm.craetivehc.com
- zerossl.crt.sectigo.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49721	20.81.200.229	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 17:15:05.695318937 CET	40	OUT	GET /x/ZGllZ28uZmVycmVpcm9Ad2l6aW5rLmVz 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: huehiufkerfpvkm.craetivehc.com Connection: Keep-Alive
Jan 27, 2021 17:15:06.061757088 CET	41	IN	HTTP/1.1 200 OK Date: Wed, 27 Jan 2021 16:15:05 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.3.11 X-Powered-By: PHP/7.3.11 Content-Length: 149 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 64 6f 63 73 2d 73 68 61 72 65 64 6f 75 72 6c 6f 6f 6b 73 65 63 75 72 65 64 6c 6f 67 69 6e 67 2e 6f 6e 6c 69 6e 65 72 73 6c 6f 67 2e 66 69 74 2f 78 2f 3f 64 69 65 67 6f 2e 66 65 72 72 65 69 72 6f 40 77 69 7a 69 6e 6b 2e 65 73 22 3c 2f 73 63 72 69 70 74 3e 0a Data Ascii: <script type="text/javascript">window.location.href = "https://docs-sharedourlooksecuredloging.onlinerslog.fit/x/?diego.ferreiro@wizink.es"</script>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49725	91.199.212.52	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 17:15:07.762238026 CET	47	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
Jan 27, 2021 17:15:07.826288939 CET	49	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 27 Jan 2021 16:15:07 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: sscrl1 Cache-Control: max-age=14400, s-maxage=3600 X-CCACDN-Proxy-ID: mcdpinlb6 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 Authority0200130000000Z3001292359595Z0K10UAT10UZeroSSL1*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	192.168.2.5	49724	91.199.212.52	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 17:15:07.763355017 CET	48	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
Jan 27, 2021 17:15:07.827099085 CET	51	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 27 Jan 2021 16:15:07 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: sscrl1 Cache-Control: max-age=14400, s-maxage=3600 X-CCACDN-Proxy-ID: mcdpinlb6 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 Authority0200130000000Z3001292359590Z0K10UAT10UZeroSSL1*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

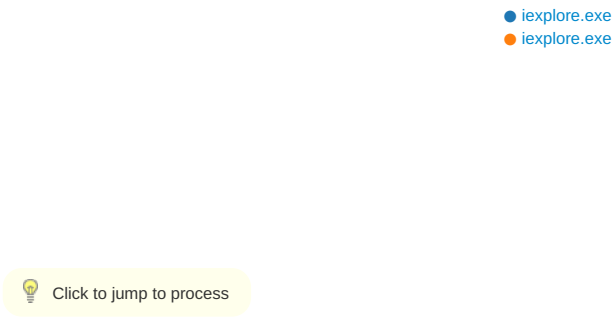
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 17:15:06.910489082 CET	40.84.135.214	443	192.168.2.5	49723	CN=docs-sharedourlooksecuredloging.onlinerslog.fit	CN=ZeroSSL RSA Domain Secure Site CA, O=ZeroSSL, C=AT	Mon Jan 25 01:00:00 CET 2021	Mon Apr 26 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
Jan 27, 2021 17:15:06.912203074 CET	40.84.135.214	443	192.168.2.5	49722	CN=docs-sharedourlooksecuredloging.onlinerslog.fit	CN=ZeroSSL RSA Domain Secure Site CA, O=ZeroSSL, C=AT	Mon Jan 25 01:00:00 CET 2021	Mon Apr 26 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
Jan 27, 2021 17:15:22.434562922 CET	40.84.135.214	443	192.168.2.5	49732	CN=docs-sharedourlooksecuredloging.onlinerslog.fit	CN=ZeroSSL RSA Domain Secure Site CA, O=ZeroSSL, C=AT	Mon Jan 25 01:00:00 CET 2021	Mon Apr 26 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 5600 Parent PID: 792

General

Start time:	17:15:03
Start date:	27/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7c33b0000
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: 5824 Parent PID: 5600

General

Start time:	17:15:04
Start date:	27/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5600 CREDAT:17410 /prefetch:2
Imagebase:	0xfe0000
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	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly