

ID: 432857
Cookbook: browseurl.jbs
Time: 21:06:10
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report http://www.7638928272.i-qlab.com/negwtod/bWxhd3NvbkBwbGF0aW51bWVxdWl0eS5jb20= 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Overview 3
Dropped Files 3
Sigma Overview 3
Signature Overview 3
AV Detection: 4
Phishing: 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted URLs 7
URLs from Memory and Binaries 7
Contacted IPs 7
Public 7
General Information 7
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 8
IPs 8
Domains 8
ASN 8
JA3 Fingerprints 8
Dropped Files 8
Created / dropped Files 8
Static File Info 15
No static file info 15
Network Behavior 16
Network Port Distribution 16
TCP Packets 16
UDP Packets 16
DNS Queries 16
DNS Answers 16
HTTP Request Dependency Graph 16
HTTP Packets 16
HTTPS Packets 17
Code Manipulations 18
Statistics 19
Behavior 19
System Behavior 19
Analysis Process: iexplore.exe PID: 328 Parent PID: 792 19
General 19
File Activities 19
Registry Activities 19
Analysis Process: iexplore.exe PID: 5268 Parent PID: 328 19
General 19
File Activities 19
Registry Activities 19
Disassembly 19

Copyright Joe Security LLC 2021

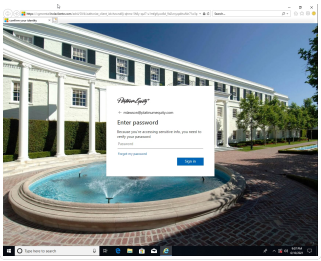
Analysis Report http://www.7638928272.i-qlab.com/neg…

Overview

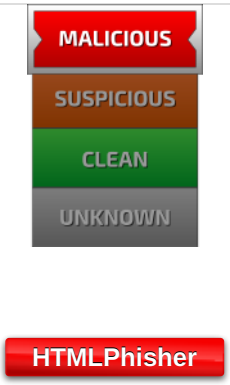
General Information

Sample URL:	http://www.7638928272.i-qlab.com/negwtod/bWxhd3NvbkBwbGF0aW51bWVxdWl0eS5jb20=
Analysis ID:	432857
Infos:	

Most interesting Screenshot:



Detection



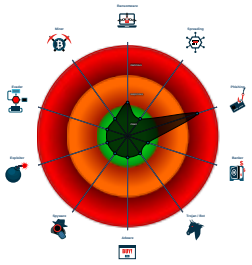
HTMLPhisher

Score:	72
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 HtmlPhish10

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 328 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5268 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:328 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\authorize_client_id_chzwnd8j-qhms-5h8y-qul7-u1mfg6ywz8xl_9d2vrxyqzkhuf4n71w3pjob56ia0esg8ctml1ov9nusch3d0pekq82btyz4l5g6wmra7jfixvmhyg37nxpde2sakzql6u5bw9fojt1r4i80c[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:



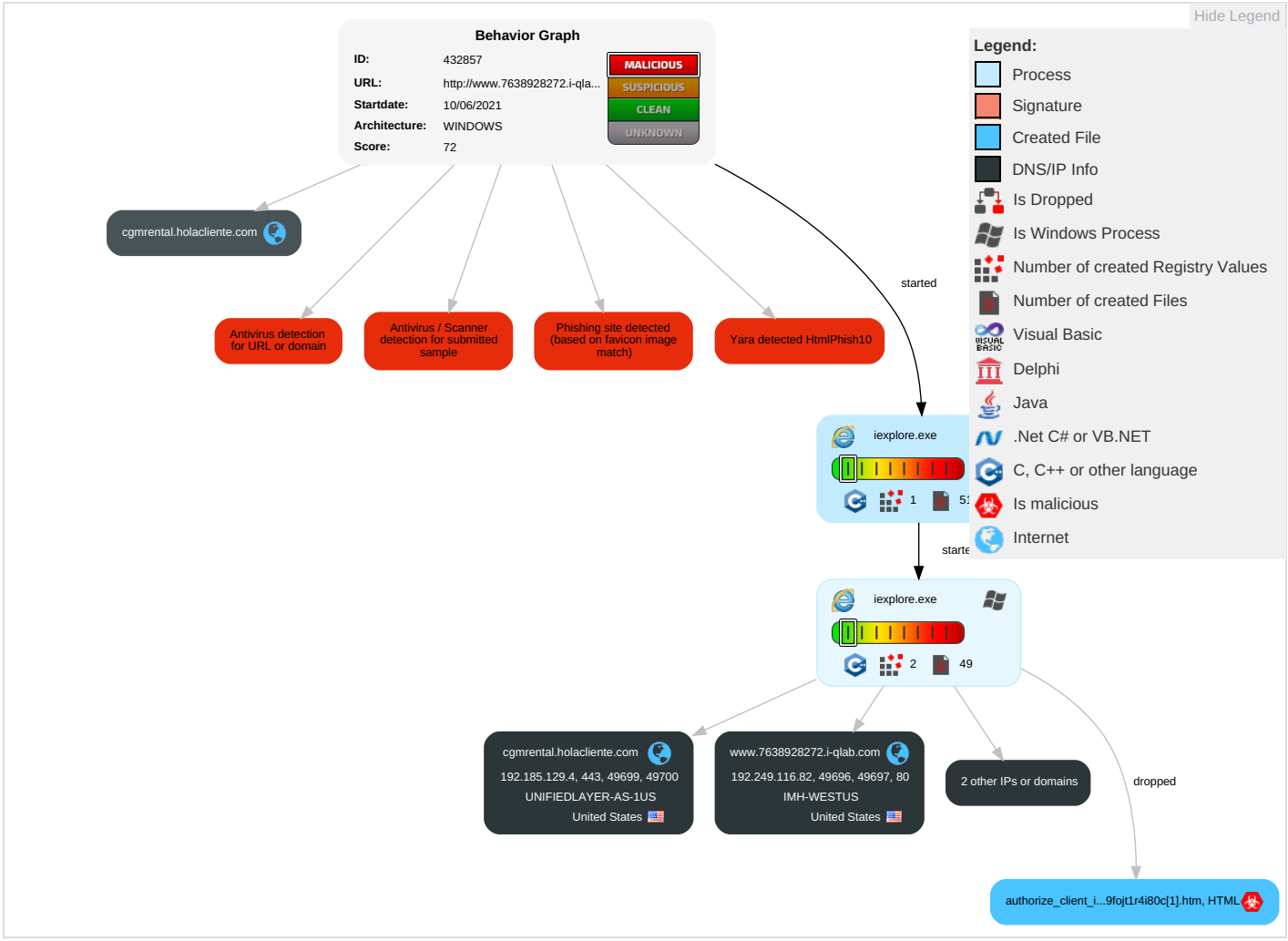
Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 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

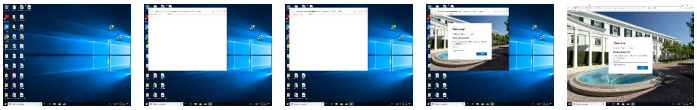
Behavior Graph

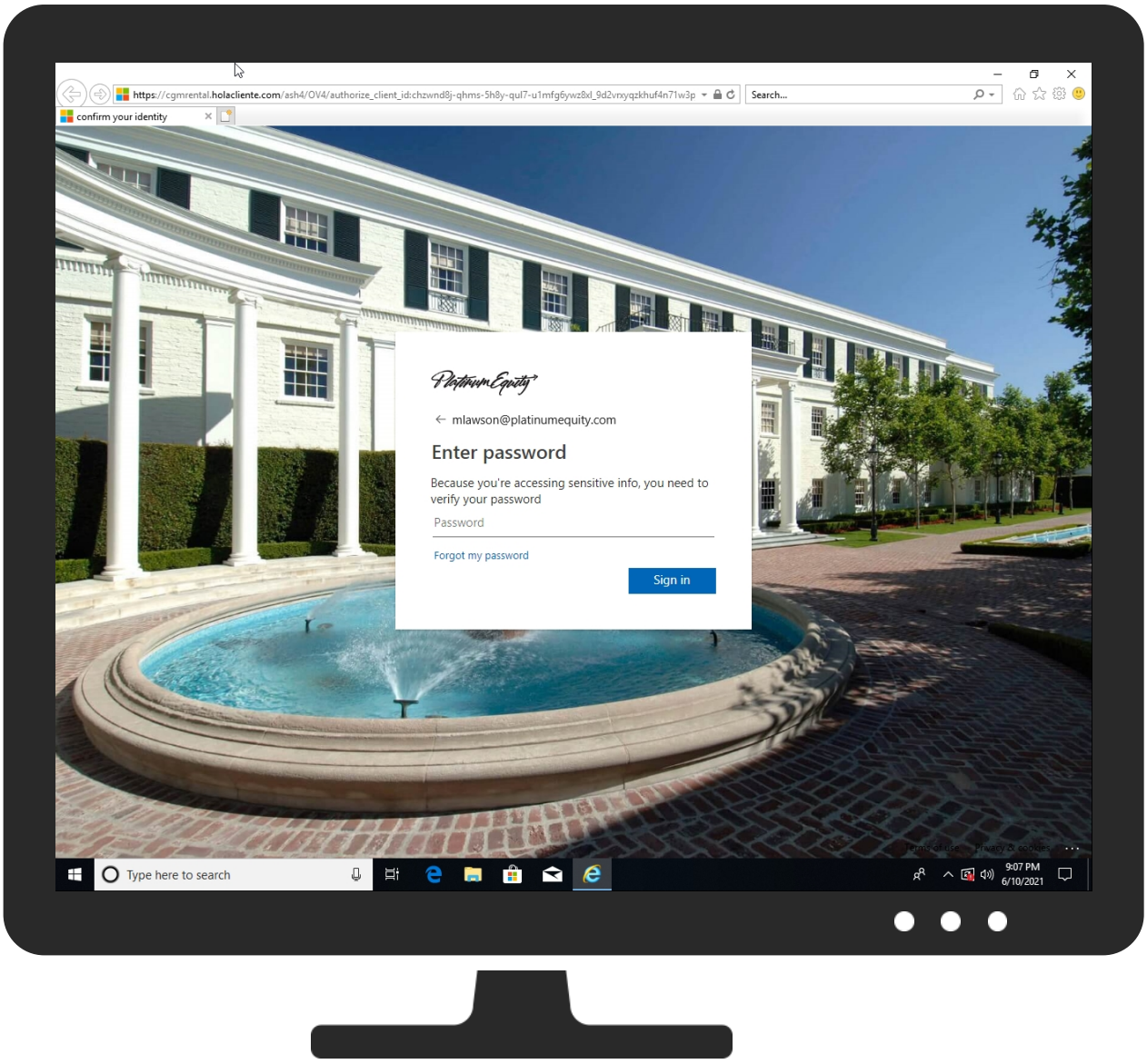


Screenshots

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://www.7638928272.i-qlab.com/negwtod/bWxhd3NvbkBwbGF0aW51bWVxdWl0eS5jb20=	0%	Avira URL Cloud	safe	
http://www.7638928272.i-qlab.com/negwtod/bWxhd3NvbkBwbGF0aW51bWVxdWl0eS5jb20=	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cgmrental.holacliente.com/ash4/OV4/authorize_client_id:chzwnd8j-qhms-5h8y-qul7-u1mfg6ywz8xl_9d2vrxyqzkhuf4n71w3pjob56ia0esg8ctml1ov9nusch3d0pekq82btyz4l5g6wmra7jfixvmhyg37nxpde2sakzql6u5bw9fojt1r4i80c?data=bWxhd3NvbkBwbGF0aW51bWVxdWl0eS5jb20=	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://www.7638928272.i-qlab.com/negwtod/bWxhd3NvbkBwbGF0aW51bWVxdWl0eS5jb20=Root	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauthimages.net/dbd5a2dd-xahzdxkxsnzqmxzzxchyicgv6e6hhqsxb5qphb4dwrw/logintenantbran	0%	Avira URL Cloud	safe	
http://https://cgmrental.holacliente.com/ash4/OV4/images/favicon.ico~	0%	Avira URL Cloud	safe	
http://https://cgmrental.holacliente.com/ash4/OV4/bWxhd3NvbkBwbGF0aW51bWVxdWl0eS5jb20=	0%	Avira URL Cloud	safe	
http://https://cgmrental.holacliente.com/ash4/OV4/authorize_client_id:chzwnd8j-qhms-5h8y-qul7-u1mfg6ywz8xl_	0%	Avira URL Cloud	safe	
http://https://cgmrental.holai-qlab.com/negwtod/bWxhd3NvbkBwbGF0aW51bWVxdWl0eS5jb20=cliente.com/ash4/OV4/au	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.7638928272.i-qlab.com	192.249.116.82	true	false		unknown
cgmrental.holacliente.com	192.185.129.4	true	false		unknown
cs1025.wpc.upsiloncdn.net	152.199.23.72	true	false		unknown
aadcdn.msauthimages.net	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.7638928272.i-qlab.com/negwtod/bWxhd3NvbkBwbGF0aW51bWVxdWl0eS5jb20=	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
152.199.23.72	cs1025.wpc.upsiloncdn.net	United States		15133	EDGECASTUS	false
192.185.129.4	cgmrental.holacliente.com	United States		46606	UNIFIEDLAYER-AS-1US	false
192.249.116.82	www.7638928272.i-qlab.com	United States		22611	IMH-WESTUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432857
Start date:	10.06.2021
Start time:	21:06:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://www.7638928272.i-qlab.com/negwtod/bWxhd3NvbkBwbGF0aW51bWVxdWl0eS5jb20=
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:	5
Number of new started drivers analysed:	0

Copyright Joe Security LLC 2021

Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.phis.win@3/22@4/3
Cookbook Comments:	• Adjust boot time • Enable AMSI
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\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{77C7E401-CA6A-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8466161535321242
Encrypted:	false
SSDEEP:	96:rOYZkZZU02bvWQOtHbfzfIKMbgq3mQQxfvfN6X:rOYZkZZU02bvWQOt7fzVMHHefvsX
MD5:	44418098CDD36261BAC20200C285F79C
SHA1:	447033D035ED91E6FEA9DAEEC0DD45EAF0A3DB8F
SHA-256:	0E189F41092919153361A3BB5424B29387F542DFF2362A99E6F5AC4C9A7F11A0

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{77C7E401-CA6A-11EB-90E5-ECF4BB570DC9}.dat	
SHA-512:	62C76AC9B7460EAAA9761284C6CB546A872F48964D175A08DF7962648C87801FCB634B4E0BE6E6A3EA8CF3DE4EDF1096954CAB7E5BA1F10DC2C064C4F7CFEF A6
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\{77C7E403-CA6A-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27284
Entropy (8bit):	1.7561822356139758
Encrypted:	false
SSDEEP:	48:Iw4Gcpr1GwpalG4pQVGrapbS/GQpBqGHHpcYcTGUp8GGzYpmifGop90iOT+zGKNW:rMZfQ36FBSpjx2FWqMSTP6+lZQ+v972r
MD5:	EED5D79ADFEC53A7775A4A4B2135FDA8
SHA1:	77B67B23712D1D75ADB55E52E9147A030E151CF7
SHA-256:	10551A2DFB5ED85EB7D4B3076AF07BABB1A3E3C4C3476425AF5B4B9FAAE167A2
SHA-512:	503A6952A819F74385F029AA498DB0C5A05D96BBABF853BDEA836173B4648F791365B827220C03C34FAD499C3C828E03AA81397131A68EF8ED847ED3A1820931
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\{7F5F0021-CA6A-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5652034241473245
Encrypted:	false
SSDEEP:	48:Iw+GcprDGwpaWG4pQWGrapbSFGQpK+G7HpRJTGIpG:riZdQm6YBSvA5TvA
MD5:	A0F613CBC4BD367E814259166936C331
SHA1:	C7244088833765A4344EB055B07D0B3BDC4010E9
SHA-256:	29504FBFC3452B8163A2D093EE033B4DCA453F2802561D5362974D6A613B1458
SHA-512:	A730559B9F67DF385D36A4748A16757DA9FF720152E70C67A0CFF5769382BCBDE75C467FF89CCB237033BD7250E14C58745AD63766B7395F3867379E6DB89F3C
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:	modified
Size (bytes):	1310
Entropy (8bit):	4.97446781072476
Encrypted:	false
SSDEEP:	24:2ZFl0yQOyrQZ9FjFjFjFAZ4qCYORlzi+fzi+fzi+fziAVR9BVK:2O5OyoBBB6ZvORlzi0zi0zi0ziGR9y
MD5:	2867B87E9A656858C1F52443BD6F06E0
SHA1:	109D55254F6991CB025921CD03A1A95BA0BDE532
SHA-256:	4E5BFA448253F5B89E92857BC5A73D31986CC2D1BC5125601FC228E4B22102EA
SHA-512:	62E2BCCCC710B9A7B6F72CDAEDE1385263FE69E11F9C31F266818D9B01848C1222E259C5B53777F31F8EFFB8552F220A43B1EA9CC374988BB46F316FFCC6898
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\dikxvqf\imagestore.dat	
Preview:	=.h.t.t.p.s.:././.c.g.m.r.e.n.t.a.l...h.o.l.a.c.l.i.e.n.t.e...c.o.m./.a.s.h.4./.O.V.4./.i.m.a.g.e.s./.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... ....P..$..%..%..%..%.. "...}.....9e..<h..<h..<h..<h..;f..c....2.....f.w....K...N...N...N...N...L..Iq...3.....g.w....L...O...O...O...O...N..Jr...3.....g.w....L...O...O...O...O...N..Jr... 3.....g.w....L...O...O...O...O...N..Jr...3.....g.w....L...O...O...O...O...N..Jr...2.....f.u....I...L...L...L...L...K..Gp.....g...i...i...i...i...f..... .....f...g...g...g...g...e.....g..i..i..i..i..h...../.....j...d....{...}...}...}...}...}...|.6..0.....k...f....}.....~.8..0.....k...f....}.....~.8..0... .....k...f....}...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\arrow_left[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:	AA3DDAB0A1CFF9533F9A668ABA4FB5E3D75ED9F8AFF8A1CAA4C29F9126D85FF4529E82712C0119D2E81035D1CE1CC491FF9473384D211317D4D00E0E234AD9F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cgmrental.holacliente.com/ash4/OV4/images/arrow_left.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-.594.594L6,12l4.944-4.944.594.594L7.617,11.578Z" 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\4PB7FJMT\firstmsg1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 353 x 41, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	3372
Entropy (8bit):	7.90561780402093
Encrypted:	false
SSDEEP:	48:akK0iImj1oaWNTm9Nu4Und08QwVu4IrwfrRUN1t4VQ5sjSPJEGNjqLNecGyuSWn9:LRbSVWN6GCwVwikjsa1MctS41FXi4
MD5:	B7EA3983E3C2D7E5F61B8D1B42758189
SHA1:	FE0817947CA4BC53152ED9378470675D9AF189FD
SHA-256:	7B6CF23AC2454B039DDF4F51B7074636ED5B08B6A1D254A47430C4ACE2A3569D
SHA-512:	6B8CD1CD56B4FF84FCAC4F605558AE32B5EF713CFA42EEDE35B7EA0E0737C53B084FB308185422D3515C4C1BD6B5A6426A65BB0D66DEC54B4AB3F018DDBB7FB7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cgmrental.holacliente.com/ash4/OV4/images/firstmsg1.png
Preview:	.PNG.....IHDR...a...).....b....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.=R#=..{.;.m..K.....p..~....3..-.09.M.h..!x.[.L.F.....Ty.{F?.....a.....7..0...a.0.-bF.0.c.....N..`O..+.....{S...9.~s.7k....6N.....N.o..x..1...../.m.5.s.t.....>._....n.?](=.....O....}}..N.....s}.....,o..Ml...g.....Ox.....4.....-I.{...j.>.S~Nsr..=./?..%V.....u^...,T...l..?..._G.m..R. ....@Z..%.V.H.Z.=u:Yf...a.. .Z.O..^.....*j..}.._^.W..J...d...$...a..!...d.[dZO...NB..d.u]2rp.j..]....;)..#..s.].<.>Y.....R.&..l].W..d.0?...6.*..n..X..#..^r.T]N.yj~|..n..Q.....E>.8.....,.... k.wMb.....(-Q\.h..c.....:R.A?.k....z...B...u.*M.....b^.:.t.....C.....oA.....>V..Bu....g..}].r....nD....~.#!.....mC.<.t..E.....T.7.ma&<..`.....4.G.....a...sx...-,...;%..g.x. ..7.s....FKx...wb....T...t9..B.y6^..T....Q.....q...../@....`6..H..c8....Q...Og#U/....G.0Z>.S_I.k....Z..0.X.....2.....0Y.u }.7.Fb.=8<t+...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\inv-big-background[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1920 x 1080, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	174883
Entropy (8bit):	7.933595362471097
Encrypted:	false
SSDEEP:	3072:NCe5AF33GgclaMBMtNxgFlxIUtjFJlj6lTmE/ORHhAFPy+huXdVnwNAH:NTOFeKtN6DIUtjdl3TgoyH
MD5:	62DDD263C8A6A4C9074E205B91182D04
SHA1:	1B56D11B012DD79DD99212EBB54ADCFB60920A9D
SHA-256:	A59EA699D353D00FF2999111F9FA11FB73A47EDA7800642609CA230560EA3703
SHA-512:	0BDAE93DDE9753BB7FB2B80B63226F3AC04F9CF58D3F954F0E9B8900F4AE5971D3B1270D4E5101E9A346B218689F7A40D70823683FBB719248A53648C02648F2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cgmrental.holacliente.com/ash4/OV4/images/inv-big-background.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\inv-big-background[1].png	
Preview:	.PNG.....IHDR.....8.....1q...bPLTEqart]c)L.qpwC..ykfX...pC.xHw`..m.JQ.7M.IYK..th.r..?...j<hW}e...lKit...^T....S..r@M.gUouZ.XR.?..m.!J.h;.k..i.+K.@..m..ZQ._U.WQ.K.. .mB._..g..l.|\.._Vog.M..JQ..k..h..cL8M.c..Z..~^..c.RP.._.fX..nJ.xS>L.dn.gV...j.`..c._~.ZU..e.eU..i.{|r5N.Zu.0J..ye.b..g..b@S~..e.{.{.\lqZ..a.ITcNN.?L..`..d.v[.xXVHM..g..u X.e:.d.aQp.{^.d..g..zg.e.XO}k...f..d.<...c.u.tvVV.c7.....vtRNS/.-.-/.-0/&.-/-,/*)//.-1.20--0/.*-&")*)/-*.++11,+-)+*.&-(.,/-./.*/*000-,-)/0/-*+/-,***/*.*+++000+,-,$-*/)0,**,'0&(,)!.Y]$.... IDATx..A..0.Eg.;..U.d....9....._..%..(.p.$.....}.....yg.vV...V.A<.WW..V...yP.5....5...F}Y.|..|...?*.`...M...6'.....<w..x.a;'..=.5....l...\....].On.l[gdg....|^.YO....x.LE..p...._.....0.$..Ky..*L ...]m]...v..!.IL.[..#x.uz..^M(...A.RE..';..e..|.#.<b}..J..GC...0i.[.[-ZW/._P8....M.,.....q.....dg...B.*Q...M.|.j...XwD....d.bJ..../....._.....z5.P...}.....^...K..=rH..k.p%g...+:..-}_..6. ..^%0.z.V.n..C#.a....y....`...h...{.%.{..05.1ry..p..'.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\passwrd[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 69 x 34, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	902
Entropy (8bit):	7.5760721199160015
Encrypted:	false
SSDEEP:	24:D8kvmvmvmvmvmvmvmvp/Hsj2lruKpPUjMFp5z/xkvAVtaWpX9gCEQ:D8mYYYYYYYRMquHnn5OvIaK8Q
MD5:	4F2A1D382216546E2C3BC620497FD4E3
SHA1:	F785EC5967B5666387304F779306F9C3E3359FF4
SHA-256:	105C03D3360CDB953585482374B2CC953D090741037502B0609629F5BB0135B7
SHA-512:	6307ADD035382E50C1B8751E567810AF9C258D8A126C536A9582D2B80C6BEDB87308E991519C7BA07041B9F108C058FF80D90BCC3E36E1FA965C287097522473
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cgmrental.holacliente.com/ash4/OV4/images/passwrd.png
Preview:	.PNG.....IHDR...E..."......|.....sRGB.....gAMA.....a.....pHYs.....+.....IDAThC.r.0...n.....e1..#..E.....a....aX..o.-.r..c.~3.....3....L.-... .. ..OcH.4. [.TNo..H.....X.Q..v.X.e{..T..i.n.e{..w..u(.w.0|6.2s.K#.?.'r....".X.S...J:...v..A.P.c;>...1..;.lLc.d.m....d.H....2.M..x.7|..C.{.<.e8a{.n...P.+.ZJ....zi.....z/...C..?...-..3..cw=a.?.....YJ}> ..XFpQ...n.i..ZJ.Un....D...kZ+C.>6.....gCY.....(....32...l.g.^.MJ0{.L.#...s.F:.;.p]..(.`.....F1%..w...."#.Y]..  ..}..T..X.n0..=8.e0N..{0.v_!.#n>....n.x..u.....R.L..=...y..n.e...|&.Y.. ..g..7...<gN.1Z..:.C..k..."..W|)Z...[u.*.Qf.JHq.V.J...GxnA...0..'.v..'....e....c. ...M.`SR.qn.k.....n.Wm.p..&nJb.{....UE.....^.m..?..w..T..#._....g..p.L.....V.H....a..6[.c...8.....x.....6.. =.....J.c..R.7W.....O.....x..x..x..x..x..x..x..x..|.....Z=..z....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\sigin[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 108 x 32, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	736
Entropy (8bit):	7.584671380578728
Encrypted:	false
SSDEEP:	12:6v/7KF/hTNSsk9V/G4ifz5SwtGfgzKf8v2zbuht0NNCXxT52FBrORsnwClc:N09NG4iL4WGfgqo23v6XRW1CI7lc
MD5:	681B83E88BA6AACCC72705FBF9F2257B
SHA1:	D69957C47026108511225160BE9BD15788D26E14
SHA-256:	F32A760F15530284447282AF5C7D0825BABF8BC4739E073928F6128830819F7A
SHA-512:	393795EAC16AFBEFA38034360C7C886FEA65016A5CEB55E1A91718474B0AE8F3AE7DFC0EA7F6C1C97334C1C6269B702A1C85236A398B78E16D19E696F213521
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cgmrental.holacliente.com/ash4/OV4/images/sigin.png
Preview:	.PNG.....IHDR...l... .....sRGB.....gAMA.....a.....pHYs.....+.....uIDAThC.AK.A...)Th...!...^....x.....S{K.'.O...['...K".I.K...Pj.B(T.$...tf..M"....}?.2ofv..?...!.z...;.+0A.c.... ..."..3D0f.`....1....Z..M..!g_U.p.....X..aX...Y.+../K.91l9{.....h..>...;..."..P..V..*.">Cv....8.$.V.8.%.v..bJ...Sw:c..]D:.LcT.6...[.}N.wi....1.t.#....O.a..E.....|...n.p..i....v.3..$.^...|.;-e;s.g..Y. F...c......u. .L.....1jd.h.w&v6.T.>..A...nXVk|i..{Wx..1.i}a...n.5]ok....<...z..+h..3U=n..OqX.j.....j.....m.x.E..|T.U..LFK0.....:`...of....c....._.Kgb.Z.I.C...wu.\.>u.]..z00+....4... ...7.!.0.2K.XY...O:.Rw...M..7...y...3.FtBb.....3...7....D..e.|....!1x.`....!.1C.c.....".+...|..z.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\bWxhd3NvbkBwbGF0aW51bWVxdWl0eS5jb20=[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	220
Entropy (8bit):	5.273695711980902
Encrypted:	false
SSDEEP:	6:hjQL/sGcQ2WF4ZXR0AqJm7+mmHFtL+3Rq9s+KqeYL:hjxbjPqJm7+xHF5kzRqdL
MD5:	58CE454957CE28AF69A4A1BAC8F9C042
SHA1:	A5ABED3171A8DE0E684C72391B5FCC2985EB5137
SHA-256:	7FA1239E8F9C3C3851F9984FD4618BEBE83173916D116CC02C48452A412E4735
SHA-512:	C972F662D18123A3EEC3FDAA11B142473E6AABB68F3F9566FA87253D2BD0CF69ED1F2CA122D1D61895D8F81C885999F70A39545BCB066C1CB4615B745E5A166
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.7638928272.i-qlab.com/negwtod/bWxhd3NvbkBwbGF0aW51bWVxdWl0eS5jb20=
Preview:	<!DOCTYPE html">.<html>. <head>. <title>Review: 0ffice365</title>. <script type="text/javascript">window.location.href = "https://cgmrental.holacliente.com/ash4/OV4/bWxhd3NvbkBwbGF0aW51bWVxdWl0eS5jb20="</script>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\enterpass[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 170 x 29, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	1446
Entropy (8bit):	7.796535000569005
Encrypted:	false
SSDEEP:	24:5CytrnsaVZjZ6+qQALzcF6zSyf/UTR8F2DFHTT6bFol73+M2XdU4:5HQaVZ/qQ7Quyf/UVIb+J3+MqU4
MD5:	BD6E291A9A3CC17ED37605E4FF0010CC
SHA1:	6C1EFD74231E3D253E0F51E4656ECED2F3335D71
SHA-256:	706DE242E7C3CFC4B16BA8174723F26FB80566C3171E9E795F057476011A5DE1
SHA-512:	D940D950167404FE53BD6A7AABAAA8C57AC58878AAD045B9F09B1FA331743A8DB5ECA2568F7E1C3D92EDA4C3AC8F1BE11240917102862F65BB0372EE1D82B33
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cgmrental.holacliente.com/ash4/OV4/images/enterpass.png
Preview:	.PNG.....IHDR.....`.....sRGB.....gAMA.....a.....pHYs.....o.d...;IDAThC.Y/..<.~?..T..U..B..PU(T?...U.Z.BUUU..PU.I23.@`.z....n.f&.?....+..U.Ec...X._.....E.....o...2.Y.Gw9.Y.....+.5....np..a...X._4~_~i...E....`..k...)....z>$..?....~. =.b.F.....8.k..X.....k.".#3.....8D5&N.V.....m.Q..7h.S.rhp...t.`.....0.L.q...9|JO.pp.Nzl...X..i...C..L..R..D.....2.n..6.....\.F.....o....9..8.ZJ...S...K..5...yz.6.FF.45q.X..?.....E/..Z...;.....A.7.^/..Y...S....4.....nE".B.....gA..(r..@N.6!>...).g..;mu....9..3.`....G. .i.ak.}`(D.!.4.g.OLb..{..#..e.....%.s....O.....Y..<li.Dd.=...a..Y.5.x.;l..J.....[Pp....:.Yhc?..U...9.aD./:.\@w.x..4=....8.}s0L|"..O.UB....ls3E.fT3.. X0+..7.....[.@.....|i..:.yF....E..O-...Z.....:>..s.VO.83.t+.(!..b<.qB1I...p...\mo.....)..)O~..?..U.E..`o...lvE}..tU",...V.v).....K..S.x.....tL.3..k!..u+.....k.C....S{.N`._.%./..r#.}._.N.N.]`.|..j..O.qV.a.....V.....03.....k..T:a...;...&. =G..qkr.<..&..`.c'.Pk..''o

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	96336
Entropy (8bit):	5.237139828082104
Encrypted:	false
SSDEEP:	1536:qUBpw+kGaazA/PWrF7qvEAFiQcpm7tEGyf5c:qiS7yfC
MD5:	9F94F80A5DC09BB962778175292195BC
SHA1:	A7F2E32B422AC9654F39EA870E403599791FCE1C
SHA-256:	1CF4B3AD7ABF3189E78C1B3BD07308C92A03FA795FDBC5821FCDE24030CFEAD0
SHA-512:	85BADDE06E879CBF558163B123BD6A35D58498F15013B981EDB849699C31FC1915B2494595C6FF0E146365413E007C2D3AB32BC83AC70632E64EE08B2B040E44
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cgmrental.holacliente.com/ash4/OV4/css/style.css
Preview:	html{font-family:sans-serif;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background-color:transparent}a:active,a:hover{outline:0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:700}dfn{font-style:italic}h1{font-size:2em;margin:.67em 0}mark{background:#ff0;color:#000}small{font-size:80%}sub,sup{font-size:75%;line-height:0;position:relative;vertical-align:baseline}sup{top:-.5em}sub{bottom:-.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr{-moz-box-sizing:content-box;box-sizing:content-box;height:0}pre{overflow:auto}code,kbd,pre,samp{font-family:monospace,monospace;font-size:1em}button,input,optgroup,select,textarea{color:inherit;font:inherit;margin:0}button{overflow:visible}but

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\ellipsis_grey[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):	3.8525277758130154
Encrypted:	false
SSDEEP:	24:t4CvnAVRfFArf1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUV0Uv6f1QqCWbVHTVeUVx:fn1r1QqC4GuiHFXS1QqCWRHQ3V1QqCWz
MD5:	2B5D393DB04A5E6E1F739CB266E65B4C
SHA1:	6A435DF5CAC3D58CCAD655FE022CCF3DD4B9B721
SHA-256:	16C3F6531D0FA5B4D16E82ABF066233B2A9F284C068C663699313C09F5E8D6E6
SHA-512:	3A692635EE8EBD7B15930E78D9E7E808E48C7ED3ED79003B8CA6F9290FA0E2B0FA3573409001489C00FB41D5710E75D17C3C4D65D26F9665849FB7406562A406
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cgmrental.holacliente.com/ash4/OV4/images/ellipsis_grey.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path fill="#777777" 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,.607.607,1.161,1.161,0,0,1,0,.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-.607A1.107,1.107,0,0,1,8,6.857m6.857,0a1.107,1.107,0,0,1,.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\NUEPGTR9\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 16x16, 32 bits/pixel
Category:	downloaded
Size (bytes):	1150
Entropy (8bit):	4.895279695172972
Encrypted:	false
SSDEEP:	24:NrQZ9FjFjFjFAZ4qCYORlzi+fzi+fzi+fziAVR9:NoBBB6ZvORlzi0zi0ziGR9
MD5:	7CDD5A7E87E82D145E7F82358F9EBD04
SHA1:	265104CAD00300E4094F8CE6A9EDC86E54812EAD
SHA-256:	5D91563B6ACD54468AE282083CF9EE3D2C9B2DAA45A8DE9CB661C2195B9F6CBF
SHA-512:	407919CB23D24FD8EA7646C941F4DCEE922B9B4021B6975DD30C738E61E1A147E10A473956A8FBB2DDF7559695E540F2CDF8535DB2C66FA6C7DECDA38BB1B12
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cgmrental.holacliente.com/ash4/OV4/images/favicon.ico
Preview:	..... .h.....(..... ....P..$..%..%..%..%.."...}.....9e..<h..<h..<h..<h..;f..c....2.....f.w....K...N...N...N...N...L..Iq...3.....g.w....L...O...O...O ...O...N..Jr...3.....g.w....L...O...O...O...O...N..Jr...3.....g.w....L...O...O...O...O...N..Jr...3.....g.w....L...O...O...O...O...N..Jr...2.....f.u....I...L ...L...L...L...K..Gp.....g...i...i...i...i...f.....f...g...g...g...g...e.....g..i..i..i..i..i..h...../.....j...d....{...}...}...}...}...}...|.6..0.....k...f....}..... .....~.8..0.....k...f....}.....~.8..0.....k...f....}.....~.8..0.....k...f....}.....~.8../.....j...e....|...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\forgpass[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 121 x 20, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	713
Entropy (8bit):	7.532865305314849
Encrypted:	false
SSDEEP:	12:6v/7WGu/MYrBNPY+iJy9aiXYgAITAmdQWjCxKy8wQg+dBH6m67tjtbYjGNgUFu56:3TrBNP7iJy9adGrQWjoDZOSUGNB4vOOm
MD5:	B19CAC60E41C79BD974C1080088C6FEF
SHA1:	FFE553D8CA430DD309494E910A989271648A4DDD
SHA-256:	E29DB32031DC537AEE9CB557B408395F3324F1E0F744349C0CDF943A3AF39296
SHA-512:	04169E96DD18AA3BB6A56D60388D05CEF24418CB109A7613E2378F275E65BE57A1D4057E12BB90126A07CAC89578830A66E2036835CE0817CB6E22BC11BA0A19
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cgmrental.holacliente.com/ash4/OV4/images/forgpass.png
Preview:	.PNG.....IHDR...y.....&.....sRGB.....gAMA.....a.....pHYs.....o.d...^IDATXG.V...0..C..H..-..."U....Q...]...xn.....yz+.8.;.B.z?t..C.....=.7.t9....hj...B..Q..y?.N?^^.\..} <.3%t<...R,2..D...&..s.:XAkr5,..D .J.....u.a...nl%.c.&4...k.,_..+7.B.Y.1GEyA-.....#p..b....r.nSb.....tu.F.q.^...b.B..?/.6....s4`.C.. ..5f...:._p...._.+.w...[O.S*...@.I.d0..."i..hcLA^..... <F.t...VnIEQ.7.C..2.P.^Ekhg.Hx.$...%F..%@....K..l[.Z#.cN.jZY:hg.Z.E.aYk..RvZ.....{...*.LH.[..bK.|... ..}..Z..G.*.|j.t.k.....ON..a.1..D.....$..pT.v..8.J....F.....1..!....D\y.....g..n.....# <..d.q.i!0...H>z..ZA\.-.].4.....G.....8..e..f..%Z....z.7....E...}....~.Z..^x....Q,.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\authorize_client_id_chzwnd8j-qhms-5h8y-qul7-u1mfg6ywz8xl_9d2vrxyqzkhuf4n71w3pjob56ia0esg8ctml1ov9nusch3d0pekq82btyz4l5g6wmra7jfixvmhyg37nxpde2sakzql6u5bw9fojt1r4i80c[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	18590
Entropy (8bit):	5.389966783784409
Encrypted:	false
SSDEEP:	384:1RDPGVZU6lmahr1AgdGgs8jMaztTLPAuz68MMv07e:1tGI6YK1AgdGgs8jJO8ts7e
MD5:	E9DC49E688BF35F52901FFAD4E0C7FE6
SHA1:	1B4B4E7D18691757FEC7A89047703BB76E9C8519
SHA-256:	A1CAA71CA89F2FBD2202117A1922903243F1F449F0219E2CCEC5A1D1F66E3C07
SHA-512:	404EE460D5497BCBEAB5204A300400DAE75907B265CD4021F9561593676F807844B8C5F591C65AC7A14DD8319A4848940F4489B1D52F83D73B6CCD4C98FAB6B3
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\authorize_client_id_chzwnd8j-qhms-5h8y-qul7-u1mfg6ywz8xl_9d2vrxyqzkhuf4n71w3pjob56ia0esg8ctml1ov9nusch3d0pekq82btyz4l5g6wmra7jfixvmhyg37nxpde2sakzql6u5bw9fojt1r4i80c[1].htm, Author: Joe Security
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">..<html dir="ltr" class="" lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">.. <title>confirm your identity</title>.. .. <meta http-equiv="X-UA-Compatible" content="IE=edge">.. <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=2.0, user-scalable=yes">.. <meta http-equiv="Pragma" content="no-cache">.. <meta http-equiv="Expires" content="-1">.. <meta name="referrer" content="no-referrer"/>.. <meta name="robots" content="none">.. <noscript>.. <meta http-equiv="Refresh" content="0; URL=./" />.. </noscript>.. <link rel="icon" href="images/favicon.ico" type="image/x-icon">.. <link href="css/style.css" rel="stylesheet" >..</head>....<body id="nsj2civ" class="nd l12736rx" style="display: block;">.. .... <div style="background-image: url("image

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\bannerlogo[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 187 x 51, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	9672
Entropy (8bit):	7.9658690982965945
Encrypted:	false
SSDEEP:	192:T1CWO2JXmaq2kRCaSx9ijsKZUXQx8KS26QWeEDDoJ71vQz49T86cA+1yR:Tokrq28jwm892xLNou+IR
MD5:	CB6880E0BAEF052C8AC5F7719A18FACA
SHA1:	68C3F1658C6417F212C4C6AFA9FD0017E08D60DC
SHA-256:	BB756FB5E8C91A67C07223EBE26DE2747B8F8D3C75550D07C0C1E7AB2A321CC6
SHA-512:	7E03DE1DF398B58AF13D2CB9D703D2173E3B5DE210F0CFFBEB441F34EC75D2A13CB5832916A0E024C079E9A7B255B68CC7FDEA3E687A213D8B932A0FD2ACF13
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msauthimages.net/dbd5a2dd-xahzdxkxsnzqmxzzxchyicgv6e6hhqsxb5qphb4dwrw/logintenantbranding/0/bannerlogo?ts=637097788097349036
Preview:	.PNG.....IHDR.....3.....sy.....sRGB.....gAMA.....a.....pHYs...t..t..f.x..%]IDATx^.....}_.u,..!-JJ..%J.TdW..~.P.."J.RJ*K..I...#.i.d.....s..q....?...{>g}..yo.|nQ...&.).....'.&*.....?.GfO....5..QQ)....s..)..D..g..w.9t...N.:..=..-[...`..g.._h....I.s..He.....c/]..]........I.....o....7.R..5kV.'o^...kn...S.H....X...Nq).'...$....=kf....i.....i..w.}g.Yc6n.h..3..*...K..d..d...*\..]....K..~...\!`...I\|...6m..7pV....3.33....X.13f..f..q.....].L...M..*.....%K.\|..L.....MHH0....q.*3k...p.B..0....M..=L.I.....n.`.T.../_!....F.a.....E....Q..A.....6..;..E.g....f....3.=.p$..U.4n...P..I'.:S.L&}..'5Ehs.0..e.L.G.U3.).....[L...)%).....DG.L....f.....8G..Ui.R...jG..?.....|.H$<.~...p.....-.W.N....3.4.|[.a....E..dI[.P!.%S&.g.....*%...X.pt.....a...,hc....cbt-I.3f.....4..^....jG..".m.bW %T".wyR.\9..s..f..uk.=..7....8...T.D^....s..)T...^..J..b.Y.N.yP.\.i.q|H*._...J..3..D.%....5pP.re3c.t].e7..5x.s.w..8.3&FZ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\ellipsis_white[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:	B9135D934B9EA50B51BB0316E383B114C8F24DFE75FEF11DCBD1C96170EA59202F6BAFE11AAF534CC2F4ED334A8EA4DBE96AF2504130896D6203BFD2DA6913F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cgmrental.holacliente.com/ash4/OV4/images/ellipsis_white.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,.607.607,1.161,1.161,0,0,1,0,.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-.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-.607A1.107,1.107,0,0,1,14.857,8,1.107,1.107,0,0,1,14.857,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\illustration[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1778x1211, frames 3
Category:	downloaded
Size (bytes):	267198
Entropy (8bit):	**7.9906108283964326**
Encrypted:	**true**
SSDEEP:	6144:6RYKpV8heKm8x9APbhvzNPns/t21mxuNDQorEU2duP:QvxKGNsl2w7o5mC
MD5:	A4F1F245C04018469DFF830BBDE4AA0F
SHA1:	2B8E49BA6B8BC526FCBE422B0344A059D8DA9FBB
SHA-256:	3AAF74C4B57853E34D460528F96424C09D125DB3BDFE4A76033F8297630FB466
SHA-512:	C09B33705854DB76F5B8FE56865292E16162B755AF07565764F1156ECFF3E5C78ECBEC4769DD054B4BA5A6D4BC85766D925F58E016B3EA9AE3974602769481A7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msauthimages.net/dbd5a2dd-xahzdxkxsnzqmxzzxchyicgv6e6hhqsxb5qphb4dwrw/logintenantbranding/0/illustration?ts=637098636344095834
Preview:	......JFIF.....C..... ....&"((&"%$*0=3*-9.$%5H59?ADED)3KPJBO=CDA...C.....A,%,AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA....."....%.V.r.v.e..%\.t..Z.J.F#&Y./....y..M)-.Q...Yf..u..!T....6...L7.h...5WF....M.B.\.:*.d.F..../.>]W.s{r.....#..Rjd.3.$....BI.$$.L.gt&t$.L.&\|.I!.BI...%I..RHN.....$..D.(wg....2Gt.I8..t...D..$'O.....;8.I(t..$$..I.I.'HN.:HN...I!$.I.BI.t.L.I$N..yY...t...N3.$..!$..BI"J1&.....>.O..I.K...~.G....C.;.t.....Ey.gg..t....e7.a;,.J.+..A....Am.*....r.o.;...X.<...k...]ceh...Y..`s.:(...\.....y..X.n~L...~x.h.y.M..uc'DS.....Ru.%I%"I.).....N.$..BN.:T.....;I...N..\.iC:uN.T..:q$.:q..$.:HI!...I8.zI!.!$.<$..*I8..8.RN'g.....*I<$...jI...I...:P.J..q.!$...$'HI8..P.$gH.+..|.H...:GB..Uu.....Fy.k..Y.hZ..:..Oj...k.....KF.-.G6..k?;].n.....6D..v.u..M%,Q.BL.f.j4GL.8h...\.[..z..1.....[..Z.-4`.|L..e..Ul.q=>}..+.p...wn

C:\Users\user\AppData\Local\Temp\~DF45FF1EEBBA1355C4.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39269
Entropy (8bit):	0.4673465611343843
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+DdvmiIiv0iOT+u0iOT+T0j5OMm9pA/b+Te:kBqoxKAuvScS+DdvmtmP6+uP6+TR97e
MD5:	A0E506BED948D9B30EE1C232A8367ABF
SHA1:	53939304845F7713EC03C778ACA401F2162FB17C
SHA-256:	4D2B9C09E02351A033E55A7977E9C337EE0D51726C416E8CACF74CECD6D81395
SHA-512:	29D414D8138C86A989D50B64A6A3F8AF289BF3A34CEE433D98AEBC7C0D40BAB84265136B50968D648AF82F585A371E346FAAD2173BBBE88D7E4713216247CA2
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 21:07:02.481618881 CEST	192.168.2.5	8.8.8.8	0xf8ec	Standard query (0)	www.7638928272.i-qlab.com	A (IP address)	IN (0x0001)
Jun 10, 2021 21:07:03.691385031 CEST	192.168.2.5	8.8.8.8	0x24b	Standard query (0)	cgmrental.holacliente.com	A (IP address)	IN (0x0001)
Jun 10, 2021 21:07:05.756138086 CEST	192.168.2.5	8.8.8.8	0x7bf7	Standard query (0)	aadcdn.msauthimages.net	A (IP address)	IN (0x0001)
Jun 10, 2021 21:07:21.251893997 CEST	192.168.2.5	8.8.8.8	0x314d	Standard query (0)	cgmrental.holacliente.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 21:07:02.633284092 CEST	8.8.8.8	192.168.2.5	0xf8ec	No error (0)	www.7638928272.i-qlab.com		192.249.116.82	A (IP address)	IN (0x0001)
Jun 10, 2021 21:07:03.749908924 CEST	8.8.8.8	192.168.2.5	0x24b	No error (0)	cgmrental.holacliente.com		192.185.129.4	A (IP address)	IN (0x0001)
Jun 10, 2021 21:07:05.819761992 CEST	8.8.8.8	192.168.2.5	0x7bf7	No error (0)	aadcdn.msauthimages.net	aadcdn.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 21:07:05.819761992 CEST	8.8.8.8	192.168.2.5	0x7bf7	No error (0)	cs1025.wpc.upsiloncdn.net		152.199.23.72	A (IP address)	IN (0x0001)
Jun 10, 2021 21:07:21.312664032 CEST	8.8.8.8	192.168.2.5	0x314d	No error (0)	cgmrental.holacliente.com		192.185.129.4	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.7638928272.i-qlab.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49696	192.249.116.82	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 21:07:02.844324112 CEST	180	OUT	GET /negwtod/bWxhd3NvbkBwbGF0aW51bWVxdWl0eS5jb20= 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: www.7638928272.i-qlab.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 21:07:03.383975983 CEST	186	IN	HTTP/1.1 200 OK Date: Thu, 10 Jun 2021 19:07:02 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Keep-Alive: timeout=3, max=100 Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 34 62 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 22 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 52 65 76 69 65 77 3a 20 20 30 66 66 69 63 65 33 36 35 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 0d 0a Data Ascii: 4b<!DOCTYPE html"><html> <head> <title>Review: 0ffice365</title>

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 10, 2021 21:07:04.081048965 CEST	192.185.129.4	443	192.168.2.5	49699	CN=cgmrental.holacliente.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat May 15 03:31:23 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Fri Aug 13 03:31:23 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	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=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Jun 10, 2021 21:07:04.086118937 CEST	192.185.129.4	443	192.168.2.5	49700	CN=cgmrental.holacliente.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat May 15 03:31:23 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Fri Aug 13 03:31:23 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	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=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Jun 10, 2021 21:07:05.908628941 CEST	152.199.23.72	443	192.168.2.5	49703	CN=aadcdn.msauthimages.net, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 03 22:55:38 CEST 2020 Wed Jul 29 14:30:00 CEST 2020 Thu Aug 01 14:00:00 CEST 2013	Sun Aug 29 22:55:38 CEST 2021 Fri Jun 28 01:59:59 CEST 2024 Fri Jan 15 13:00:00 CET 2038	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=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jul 29 14:30:00 CEST 2020	Fri Jun 28 01:59:59 CEST 2024		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Fri Jan 15 13:00:00 CET 2038		
Jun 10, 2021 21:07:05.908772945 CEST	152.199.23.72	443	192.168.2.5	49702	CN=aadcdn.msauthimages.net, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 03 22:55:38 CEST 2020 Wed Jul 29 14:30:00 CEST 2020 Thu Aug 01 14:00:00 CEST 2013	Sun Aug 29 22:55:38 CEST 2021 Fri Jun 28 01:59:59 CEST 2024 Fri Jan 15 13:00:00 CET 2038	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=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jul 29 14:30:00 CEST 2020	Fri Jun 28 01:59:59 CEST 2024		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Fri Jan 15 13:00:00 CET 2038		
Jun 10, 2021 21:07:21.648727894 CEST	192.185.129.4	443	192.168.2.5	49704	CN=cgmrental.holacliente.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat May 15 03:31:23 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Fri Aug 13 03:31:23 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	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=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 328 Parent PID: 792

General

Start time:	21:06:59
Start date:	10/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff67a1a0000
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: 5268 Parent PID: 328

General

Start time:	21:07:00
Start date:	10/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:328 CREDAT:17410 /prefetch:2
Imagebase:	0x70000
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

Copyright Joe Security LLC 2021