

JOeSandbox Cloud BASIC



ID: 432837

Cookbook: browseurl.jbs

Time: 20:25:42

Date: 10/06/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report https://gabriellarodriguezart.com/Dr	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	17
No static file info	17
Network Behavior	17
Network Port Distribution	17
TCP Packets	17
UDP Packets	17
DNS Queries	17
DNS Answers	17
HTTPS Packets	18
Code Manipulations	19
Statistics	19
Behavior	19
System Behavior	20
Analysis Process: iexplore.exe PID: 6828 Parent PID: 800	20
General	20
File Activities	20
Registry Activities	20
Analysis Process: iexplore.exe PID: 6908 Parent PID: 6828	20
General	20
File Activities	20
Registry Activities	20
Disassembly	20

Analysis Report https://gabriellarodriguezart.com/Dr

Overview

General Information

Sample URL:

http://https://gabriellarodriguezart.com/Dr

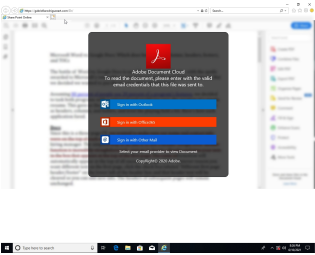
Analysis ID:

432837

Infos:



Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

HTMLPhisher

Score:

84

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Antivirus / Scanner detection for sub...

Antivirus detection for URL or domain

Phishing site detected (based on sh...

Yara detected HtmlPhish10

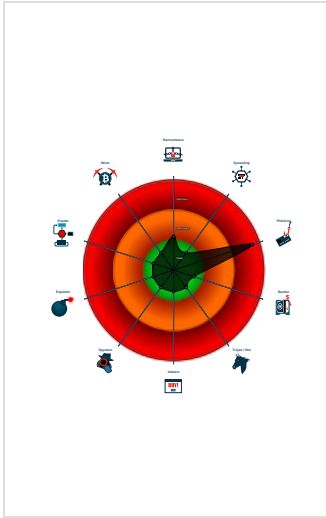
Yara detected HtmlPhish7

Phishing site detected (based on va...

HTML body contains low number of ...

HTML title does not match URL

Classification



Process Tree

- System is w10x64
-  iexplore.exe (PID: 6828 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
 -  iexplore.exe (PID: 6908 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6828 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEE8013E2AB58D5A)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\Dr[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\Dr[1].htm	JoeSecurity_HtmlPhish_7	Yara detected HtmlPhish_7	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

AV Detection:



Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:



Phishing site detected (based on shot template match)

Yara detected HtmlPhish10

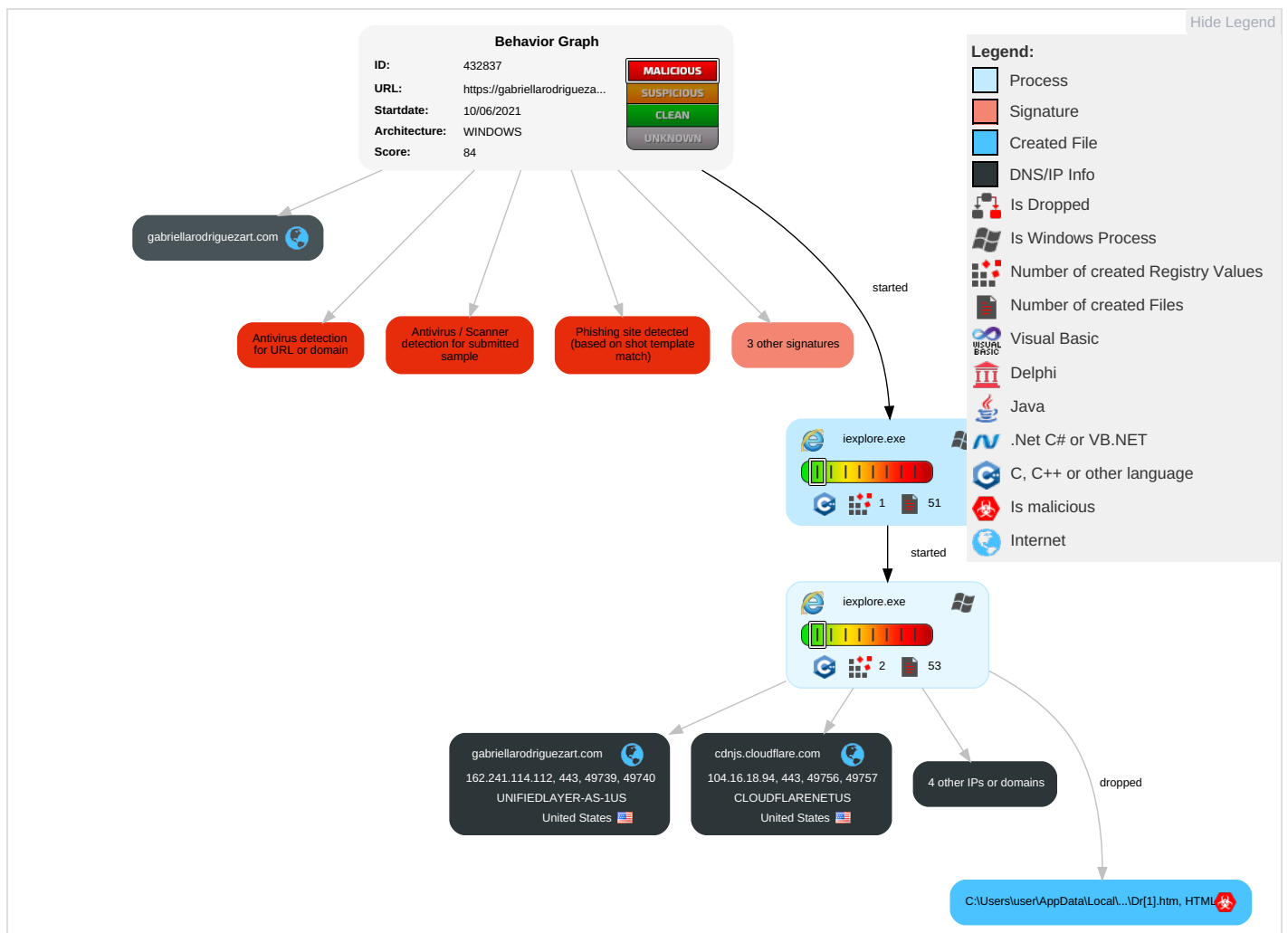
Yara detected HtmlPhish7

Phishing site detected (based on various OCR indicators)

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	Impact
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	Modify System Partitions
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 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device 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 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

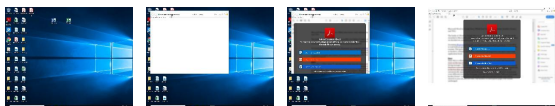
Behavior Graph

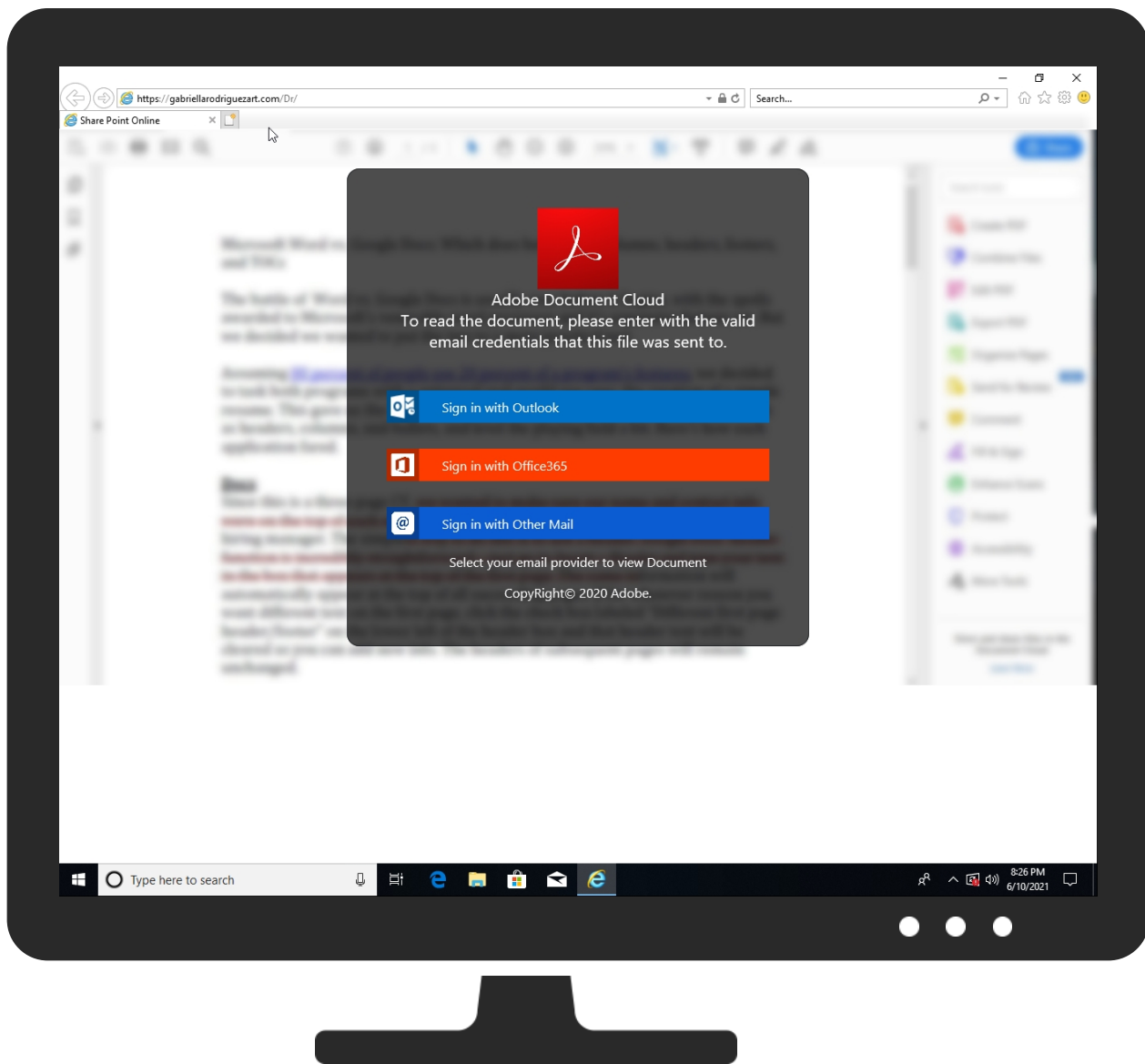


Screenshots

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://https://gabriellarodriguezart.com/Dr	0%	Avira URL Cloud	safe	
http://https://gabriellarodriguezart.com/Dr	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
--------	-----------	---------	-------	------

Source	Detection	Scanner	Label	Link
http://https://gabriellarodriguezart.com/Dr/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://ianlunn.github.io/Hover/	0%	Virustotal		Browse
http://ianlunn.github.io/Hover/	0%	Avira URL Cloud	safe	
http://https://gabriellarodriguezart.com/Dr/\$Share	0%	Avira URL Cloud	safe	
http://https://gabriellarodriguezart.com/Dr/I	0%	Avira URL Cloud	safe	
http://https://getbootstrap.com	0%	Avira URL Cloud	safe	
http://ianlunn.co.uk/	0%	URL Reputation	safe	
http://ianlunn.co.uk/	0%	URL Reputation	safe	
http://ianlunn.co.uk/	0%	URL Reputation	safe	
http://https://gabriellarodriguezart.com/Dr/Root	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gabriellarodriguezart.com	162.241.114.112	true	false		unknown
cdnjs.cloudflare.com	104.16.18.94	true	false		high
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://gabriellarodriguezart.com/Dr/	true	SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
162.241.114.112	gabriellarodriguezart.com	United States		46606	UNIFIEDLAYER-AS-1US	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432837
Start date:	10.06.2021
Start time:	20:25:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://gabriellarodriguezart.com/Dr/
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:	6
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:	mal84.phis.win@3/25@7/3
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.{5E5D7668-CA19-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8519445073708543
Encrypted:	false
SSDEEP:	192:riZ5Zx2GHWGKtGiifGWwazMGjCBGG8DGnsfGrwTjX:revAG2GCGLG3G+GBGSGk
MD5:	8CFD78B987F70DE24279106ECC30FD5D
SHA1:	18711387EA29E74B7BA4104B5FAB15B428061546

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{5E5D7668-CA19-11EB-90EB-ECF4BBEA1588}.dat	
SHA-256:	8A717F81B44DDAA879161DB55D43868F6517AD7DA0AA5A00872B28F4E8B97021
SHA-512:	B7F8837BDB459145A80C1FDEE06081161EA78E436B977F0C6B258243EA07C0D0EE85957F8645E65020053951818D578D3C031CF1A67A137D567DDE4BE98E3D18
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\{5E5D766A-CA19-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27410
Entropy (8bit):	1.770997795015822
Encrypted:	false
SSDEEP:	96:rnZEq46uBS1jFX2FWFGMFC03ZH3HSgbwr:rnZEq46uk1jFX2FWFGMFC03ZH3HSHr
MD5:	A58DBDF3DCB9A1A5EF15B00ED7E2874B
SHA1:	A75B95498B2C93AF256C542A5F602DC0A456D079
SHA-256:	7EA6C945CCE12A229C10F5004324AE9D20B696E0766F07FADE75796D712D7A94
SHA-512:	24FFB606EBCC8722979B2594C644A5968E330891CEA265F2903F55571D91D8386E0A44676EBA42039DF2307C6E5174241647A564F5814C475556F6B5BA3C055B
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\{5E5D766B-CA19-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.563917014555442
Encrypted:	false
SSDEEP:	48:lw6GcprDGwpaiG4pQWGrapbS3tGQpKlxG7HpRFTGlpG:r+ZdQS6YBS3XAlgTTA
MD5:	ABB8B868425AEC49D0438DA00D36498E
SHA1:	B64E3294D060FC48D5BD6199A4F2F47D901571CE
SHA-256:	CB3A7CA250F88A2A9F907BBDF8A8EA4DB5F535B2667C9F64EEEC5A0AC1004D9FC
SHA-512:	3A0A134E32D9191C38C46AF38010238B78F50F58AAA382A1FB0463D336BE508F04F586702DAB28EA8F8EE489873F64D6A55CCAC9A6C52D457BB3969CC3A4FE6
Malicious:	false
Reputation:	low
Preview:	R.o.o.t. .E.n.t.r. y.....

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\585b051251[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	10866
Entropy (8bit):	5.182623714755422
Encrypted:	false
SSDEEP:	192:BgHN42S+9SZRvACpilthFzoXnemF+shSGnZ+PPxQDqv7jh81Q5l8OcchlzbCn:WRCfhFzevnEZ/h81Q5l8OsE
MD5:	D8CA71772D1E86D5FB9D5E2F6CC1AE70
SHA1:	9B043E60997FE552D652E4474E16AFF923D7AA76
SHA-256:	7D840153F02AD6D91D652354E35B590721916D16C33956631EEF0E7D3B5613EE
SHA-512:	8E9DA8E9AE10EC0EB854A6E488FB4568A960EE10AF46FE4AA49F22F227CB94997F40E49E10A81E341B99489256163A2C0E065730EEA642777061CDA61B4D56C1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://kit.fontawesome.com/585b051251.js

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\585b051251[1].js

Preview:	<pre>window.FontAwesomeKitConfig = {"asyncLoading":{"enabled":true},"autoA11y":{"enabled":true},"baseUrl":"https://ka-f.fontawesome.com","baseUrlKit":"https://kit.fontawesome.com","detectConflictsUntil":null,"iconUploads":{},"id":"132286382","license":"free","method":"css","minify":{"enabled":true},"token":"585b051251","v4FontFaceShim":{"enabled":false},"v4shim":{"enabled":true},"version":"5.15.3"};.(function(t){function e==typeof define&&define.amd?define("kit-loader",t):t})((function(){"use strict";function t(e){return(t="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(t){return typeof t}:function(t){return t&&"function"==typeof Symbol&&t.constructor===Symbol&&t!=="Symbol.prototype"?symbol:"type of t"}(e))function e(t,e,n){return e in t?Object.defineProperty(t,e,{value:n,enumerable:!0,configurable:!0,writable:!0}):t[e]=n,t}function n(t,e){var n=Object.keys(t).if(Object.getOwnPropertySymbols){var r=Object.getOwnPropertySymbols(t);e&&(r=r.filter((function(e){return Object.g</pre>
----------	--

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\Dr[1].htm



Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	245
Entropy (8bit):	5.108410272788199
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwol6hEr6VX16hu9nPbTvT8OR+KqD:J0+ox0RJWWPnL8zT
MD5:	8303D52E9315425F58AEE965D469C11D
SHA1:	5F1CA9BC12AA97C9D139AC4F16552819B96733F3
SHA-256:	6ED6D06A696254FAE109940AED4455A6497B264091AF58B6B368D6E0149CC531
SHA-512:	61EE88284C89F5541D50D5BA00A9A27A3A72BD5DE27045E4D6CCEE4709BA5794D2F46EEBCC70131FFB26E995E3FBD66670D423ACF4B8C2CC1EAC511F6DBACE42
Malicious:	true
Yara Hits:	- Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\Dr[1].htm, Author: Joe Security - Rule: JoeSecurity_HtmlPhish_7, Description: Yara detected HtmlPhish_7, Source: C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\Dr[1].htm, Author: Joe Security
Reputation:	low
Preview:	<pre><!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>301 Moved Permanently</title>.</head><body>.<h1>Moved Permanently</h1>.<p>The document has moved here.</p>.</body></html>.</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\free-v4-shims.min[1].css

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	26701
Entropy (8bit):	4.829823522211244
Encrypted:	false
SSDEEP:	192:dP6hT1bIl4w0QUmQ10PwKLaAu5CwWavpHo4O6wgLPbJVR8XD7mycP:0hal4w0QK+PwK05eavpmgPPeXD7mycP
MD5:	8A99CE81EC2F89FBCA03F2C8CF1A3679
SHA1:	58F9EF32D12A5DA52CBA87BD518BCC998FC59EF9
SHA-256:	362DAEAF1F7E05FEE9A609E549F148AACBE518C166FBD96EAD69057E295742AF
SHA-512:	930F28449365FAED13718BB8F332625DB110ABB08C3778DC632FDF00A0187A61A086B5EB4765FFC1923B64E2584C02592A213914B024DE6890FF3DBFC3A12FE5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.3/css/free-v4-shims.min.css?token=585b051251
Preview:	<pre>/*!. * Font Awesome Free 5.15.3 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.fa.fa-glass:before{content:"\f000"}.fa.fa-meetup{font-family:"Font Awesome 5 Brands";font-weight:400}.fa.fa-star-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-star-o:before{content:"\f005"}.fa.fa-close:before,.fa.fa-remove:before{content:"\f00d"}.fa.fa-gear:before{content:"\f013"}.fa.fa-trash-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-trash-o:before{content:"\f2ed"}.fa.fa-file-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-file-o:before{content:"\f15b"}.fa.fa-clock-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-clock-o:before{content:"\f017"}.fa.fa-arrow-circle-o-down{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arrow-circle-o-down:before{content:"\f358"}.fa.fa-arrow-circle-o-up{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arro</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\free.min[1].css

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	60351
Entropy (8bit):	4.728641238865369
Encrypted:	false
SSDEEP:	768:0Uh31PIpyXNq4YxBowbgJlkwF/zMQyYJYX9Bft6VSz8:0U0PxXE4YXJgndFTfy9lt5Q
MD5:	390B4210E10C744C3C597500BCF0B31A
SHA1:	2600C7C2F25D7DBCBC668231601E426010DC6489
SHA-256:	C2819CA1F7AD1AF7BA53C4EDFD7395C547BCB16D29892A234D7860C689ED929
SHA-512:	E8A7E466BE8CC092E12994B51A6A8A39E2FBB66DD48221BCF499BB89365B4004D73C1909F8FE0BBBFB13907D5901D76FFE127D92FDD7493853646F83F5985CB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.3/css/free.min.css?token=585b051251

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\free.min[1].css	
Preview:	/*!. * Font Awesome Free 5.15.3 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.fa,.fab,.fad,.fal,.far,.fas{-moz-osx-font-smoothing:grayscale;-webkit-font-smoothing:antialiased;display:inline-block;font-style:normal;font-variant:normal;text-rendering:auto;line-height:1}.fa-lg{font-size:1.33333em;line-height:.75em;vertical-align:-.0667em}.fa-xs{font-size:.75em}.fa-sm{font-size:.875em}.fa-1x{font-size:1em}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-6x{font-size:6em}.fa-7x{font-size:7em}.fa-8x{font-size:8em}.fa-9x{font-size:9em}.fa-10x{font-size:10em}.fa-fw{text-align:center;width:1.25em}.fa-ul{list-style-type:none;margin-left:2.5em;padding-left:0}.fa-ul>li{position:relative}.fa-li{left:-2em;position:absolute;text-align:center;width:2em;line-height:inherit}.fa-border{border:.08em solid #eee;border-radius:.1em;padding:.2em .25em .15em}.fa-pul

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\outlook1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 26 x 26, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	771
Entropy (8bit):	7.682244426935498
Encrypted:	false
SSDEEP:	24:74yiH9yQmOntihdLI00qDeu1BcaDa0oljZG0:omOntO7v/uJDYG0
MD5:	C3FC46C5799C76F9107504028F39190F
SHA1:	519096AD3F03410CF9CE3C9B9FCCA6B439D97B23
SHA-256:	57898461712A639D119BDF88B7145919DCC8956C7A271D2E4A1084B29EAE6785
SHA-512:	DF4A0A2F78B2013035FB738BF405119B275D4CFEC31A23071EB9AF499D5F31FDC4BE22754CE791C975D7D417E908B5CAD16F962B0ADD3DFDCDE19844D74F668
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://gabriellarodriguezart.com/Dr/images/outlook1.png
Preview:	.PNG.....IHDR.....JL.....bKGD.....IDATH...k.A.k6.b.F1..H@...j@.aQ...(.....A.D...l.....E.....1...W...;:Y.d.}}.U5]..x"3?...!..A..y..+R2l...m.NX.=..p.0...d.^3.....J.Z.X.).....Pl..x1.3.M.0....m.....F.....?...n.....l.Fo)x_ R s..a.T?...?=9.Y...u...z..Wz...h..<..P...\$Y.....k'/4.y/.....L.C.....".....U...7...G...h.....1j1E..%t....@...a.....b.ED-.Tn<.o.D...o..({1>.....".4a.:k.l/./7t/./Q'->.....'3eb..d.@=4...C....A...;..N.X3.(.....v...+...S...W..l...@...j.)u<..@u..0...V&b.y.p....0..o.?..V..B =~&m"r (...6;EP.T.....h.m".[f.U)]t..2.Q....g.cP.W...D..[O>..d;:yl./!..#v..._\$.Q.....tE..Si.q..._/n...v.w..Uo ...#..S.....^.....F...+..._??f.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\adobe[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 400x400, frames 3
Category:	downloaded
Size (bytes):	30925
Entropy (8bit):	7.75667128400845
Encrypted:	false
SSDEEP:	768:nuowBuvTpjgz+wqrPZ2qh8fmyjIX6RqnxgYqwNL:nuPOpigzPqrPZRYZGnYqYL
MD5:	BE5274AF7D8BD25B8148A190FF515399
SHA1:	B8D0850FD92EE935287E17988B89E53607808C8C
SHA-256:	26C62DBDF527B8DCBF378EA62F129CBBBA3B244730687909BA21ECD729C9D2E6
SHA-512:	64893C625BE72783088575E36EF26FF4573243F32601BDA754EDA72B7515063B5E4E4831697D16AC663529C910AE12CCD145BEC530F2A9BAE4D9324301C65667
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://gabriellarodriguezart.com/Dr/images/adobe.jpg
Preview:	JFIF.....C.....".....!1A..Qa."q.2....#B...R..\$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....!1..AQ.aq."2...B....#3R..br...\$4%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..g..... ?..."+".....4...R...'.q..~...n.7.....QXJ<...=...^V'@U..E..5....Uz.....IE.PTe.)/p.y.....T.<...-T.. ...b.=.#IU..-...{O/...b..E.....X...G...?....._...M..g.....T-g.....<.....T-g.....3\$=_...IU.K..^..E...=#U..._ X.R.=W...1.....QTr..l....*7...?.6.9K.^E.Ps.l.....%W..y..g)s(KX)<.....

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\hover[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	114697
Entropy (8bit):	4.9296726009523
Encrypted:	false
SSDEEP:	1536:67O7EesvXIPRX4PT8aZv8qoXloqbTFaFeTxvyAZ+D7M71D:qXIPRX4PT3
MD5:	FAC4178C15E5A86139C662DAFC809501
SHA1:	EF1481841399156A880EC31B07DDA9CFAA1ACE39
SHA-256:	BB88454962767EB6F2DDB1AABAAF844D8A57DE7E8F848D7F6928F81B54998452
SHA-512:	0902219B6E236FBF9D8173D1D452C8733C1BF67B0EB906CC9866EA0C27C2D08F6DA556D01475E9B54E2C6CE797B230BFBD5F39055CE0C71EA4D3E36872C37819
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://gabriellarodriguezart.com/Dr/css/hover.css

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\CS6\XJW6\jquery.min[1].js	
Reputation:	low
IE Cache URL:	http://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js
Preview:	<pre>/*! jQuery v2.2.4 (c) jQuery Foundation jquery.org/license */!function(a,b){"object"!==typeof module&&"object"!==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}("undefined"!==typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="2.2.4",n=function(a,b){return new n.fn.init(a,b)},o="/^\s\uFEFF\uA0+ [\s\uFEFF\uA0]+\$ g,p=/^~ms-/,q=/-([da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,function(b,c){return a.call</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\OR0WKIO1\Dr[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	11777
Entropy (8bit):	4.8159515725639555
Encrypted:	false
SSDEEP:	192:K2FI5vEJKnYmrDfG4RywAOT+UY/t4ldtWPTy:1nmRnAKyt48tZ
MD5:	6D1D3C4FD92B63CC534BE0EDF3AF18DC
SHA1:	5F5442FEB5BE60239F185E969C45050A7DBADE2A
SHA-256:	65ADCB045AEFB4D0028A6AF36EC9D42BBD4DAE9AFF2CF85810BB4A6F44D4B25C
SHA-512:	2D42684CF0A44E262C958172C2446974A4AE9B8D17F7208A5FCB690964EE0D56FEB157B9AB6166B8F94FBD CBA027271C36B66784655E8FD96CE0B5522FE71AA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://gabriellarodriguezart.com/Dr/
Preview:	<pre>...<!doctype html>..<html lang="en">..<head>.. <script src="https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>.. <script src="https://code.jquery.com/jquery-3.1.1.min.js">.. <script src="https://code.jquery.com/jquery-3.3.1.js" integrity="sha256-2Kok7MbOyxpgUVvAk/HJ2jigOSYS2auK4Pfzbm7uH60=" crossorigin="anonymous"></script>.. Required meta tags -->.. <meta charset="utf-8">.. <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">.... Bootstrap CSS -->.. <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css" integrity="sha384-Gn5384xqQ1ao WXA+058RXPxPg6fy4IWvTNh0E263XmFcJlSAwiGgFAW/dAiS6JXm" crossorigin="anonymous">.. <link href="https://fonts.googleapis.com/css?family=Yellowtail&display=swap" rel="stylesheet">.. <script src="https://kit.fontawesome.com/585b051251.js" crossorigin="anonymous"></script>.. <title>Share Point Online</title>.. <link</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\OR0WKIO1\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	211
Entropy (8bit):	5.026484232218891
Encrypted:	false
SSDEEP:	6:0IFFwKh+56ZRWHMqh7izlpDBEoKOEETJONin:jFWmO6ZRoMqt6p3EondOY
MD5:	04F7435B2672FBE66984EA436E7087C6
SHA1:	44896875E69B297EB979CC0D3E8522D872656BA8
SHA-256:	F9088C15A062F0C7708C3864C5E261A2E4961DFEB0F150DF744FAEC2E3B74AD6
SHA-512:	9A1D01A7FAC3D6B205CFA37C05A93AFA9D903D4D35DCB16E31D3A31D19CD65B8DE5D66E626BC7F70D07841C779E20CD2C2DD6254824F96DE0E8E576E156F17D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Yellowtail&display=swap
Preview:	<pre>@font-face { font-family: 'Yellowtail'; font-style: normal; font-weight: 400; font-display: swap; src: url(https://fonts.gstatic.com/s/yellowtail/v11/OZpGg_pnoDtINPFRllO_hlvHxw.woff) format('woff'); }</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\OR0WKIO1\gmail[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1280 x 1280, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	66743
Entropy (8bit):	7.712342056984168
Encrypted:	false
SSDEEP:	1536:FxqKcVqezl0vLoYxEuKoYk5LHjGkT3b1mQOEj0+R+EH:Fsk2qezl0zoYxEuKo7CYrOb+Rb
MD5:	DCE2F2B0E50CB1DBB0246D152791CB46
SHA1:	D0A69C159304EDC08DB005163E7A0DAF5A1E98A6
SHA-256:	ACF087C1757F08B0CFD53D59066544D7EF0BFCC50999E77C5813739CD9DC1479
SHA-512:	91054B36EF1673B24E4FE3DC324CBE339F4E9EB72785A6A4C355C7B2A11A9A7C6E188FF9BF5B34FFDD2805D4BBED71EF6CA4975EE3E330FD8D8E383ED64B26EE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://gabriellarodriguezart.com/Dr/images/gmail.png

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\OR0WKIO1\gmail[1].png

Preview:	.PNG.....IHDR.....sBIT.... .d....pHYs...../...tEXtSoftware.www.inkscape.org.<...IDATx...{x.u....l.sS.9Q(.J.L&\$.V#..".Zw.eEQv.Q.U.A)9Vh..l8...H2)`...i....).f.y...L.pu...{n.....@ls....mj=...X<65...U.l.b.t.U...mR...e.P.i.i.i2U..@N1.f...i.s...cf..J....2ev.`.% .o...s.j..l.B...V&..s;b..Pfg.....!....5...\$.@...l0.=.lY.....a...B.4g...T.9Wif..R..o.R.t'.0...?G.9i...L...*.&..s.Vgnkhn...;p[.0.5.....\$.P.....^".HL.M...@.p.;04....9.&(i....9.sK.=&.\$m.....f..1.'...f2.Uww.....PH....@..xq...k.2..l.Luf..s5..`
----------	---

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\OR0WKIO1\office3651[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 187 x 188, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	18025
Entropy (8bit):	3.011161251318808
Encrypted:	false
SSDEEP:	96:2S+WvkiqJq6Uq7NXrNG+GHsc5yeFZV9D2Ydcx/NTV0K0VFDsCmm:2SjkiOq6Uq75shDs1kFP
MD5:	FE22440D79FFA34950F512EF4A718B2A
SHA1:	0E147E59544EE6580D3095353D4420849FA5EB8A
SHA-256:	A2F26B68A6C8810C1AEB4048C938F835A86BA83756A7A440F989B967E78F3BA8
SHA-512:	64218ECD4140DC05E50EB7BA4C98137948B85A4310C8308244205BA6ADA8EE7C2D1840121730A00800E41775241D8AFA02125A966064CD0EB2CC7D3E4605B81C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://gabriellarodriguezart.com/Dr/images/office3651.png
Preview:	.PNG.....IHDR.....pHYs.....<eiTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?><x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmpk="Adobe XMP Core 5.6-c067 79.157747, 2015/03/30-23:40:42 ">. <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about="". xmlns:xmp="http://ns.adobe.com/xap/1.0/". xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/". xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#". xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/". xmlns:dc="http://purl.org/dc/elements/1.1/". xmlns:tiff="http://ns.adobe.com/tiff/1.0/". xmlns:exif="http://ns.adobe.com/exif/1.0/". <xmp:CreatorTool>Adobe Photoshop CC 2015 (Windows)</xmp:CreatorTool>. <xmp:CreateDate>2020-01-18T21:49:38+05:00</xmp:CreateDate>. <xmp:MetadataDate>2020-01-21T14:30:14+05:00</xmp:MetadataDate>. <x

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\OR0WKIO1\other1[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 190 x 187, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	21882
Entropy (8bit):	4.268463452779894
Encrypted:	false
SSDEEP:	192:ESCKiDw7e9Mg/wio0EYm9FWyo2XdJfXoOZdEDfmiIJQdiRVi/WTanY:DBiDw7eAdq+FWyo2/fXoZbDIJ0ci/BnY
MD5:	6843A244E12FAB158AA189680B5E7049
SHA1:	0E1C691F87CC4FA35C88344974F2829C40176B70
SHA-256:	3A9B144D6482B78AFC4E0A940A1D3C22240F14FA535B808CF4DAB9635339569F
SHA-512:	145010C45B6B83EA4005EB367C0507959FF0817E482F19E9973504081ACAE1B7827CBD1172CEC7732B13F4E0CEC058271BD6700444FBCF61FB6A3C068A3744C4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://gabriellarodriguezart.com/Dr/images/other1.png
Preview:	.PNG.....IHDR.....\$.cHRM..z&.....u0...`.....p.Q<...sRGB.....gAMA.....a....pHYs.....iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?><x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmpk="Adobe XMP Core 5.6-c067 79.157747, 2015/03/30-23:40:42 ">. <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about="". xmlns:xmp="http://ns.adobe.com/xap/1.0/". xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/". xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#". xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/". xmlns:dc="http://purl.org/dc/elements/1.1/". xmlns:tiff="http://ns.adobe.com/tiff/1.0/". xmlns:exif="http://ns.adobe.com/exif/1.0/". <xmp:CreatorTool>Adobe Photoshop CC 2015 (Windows)</xmp:CreatorTool>. <xmp:CreateDate>2020-01-18T21:59:57+05:00</xmp:CreateDate>. <

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\OR0WKIO1\popper.min[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	19188
Entropy (8bit):	5.212814407014048
Encrypted:	false
SSDEEP:	384:+CbuG4xGN0Dic2UjKpafxwC5b/4xQviOJU7QzxxivDdE3pcGdjkd/9jt3B+Kb964:zb4xGmiJfaf7gxQvVU7eziv+cSjknZ3f
MD5:	70D3FDA195602FE8B75E0097EED74DDE
SHA1:	C3B977AA4B8DFB69D651E07015031D385DED964B
SHA-256:	A52F7AA54D7BCAFA0A056EE0A050262DFC5694AE28DEE8B4CAC3429AF37FF0D66
SHA-512:	51AFFB5A8CFD2F93B473007F6987B19A0A1A0FB970DD59EF45BD77A355D82ABBBD60468837A09823496411E797F05B1F962AE93C725ED4C00D514BA40269D1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\OR0WKIO1\popper.min[1].js

Preview:	<pre>/* * Copyright (C) Federico Zivolo 2017. Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT).. */(function(e,t){'object'==typeof exports&&'undefined'!=typeof module?module.exports=t():'function'==typeof define&&define.amd?define(t):e.Popper=t()})(this,function(){'use strict';function e(e){return e&&[object Function]==={}?e.toString.call(e):function t(e,t){if(1!==e.nodeType)return[];var o=getComputedStyle(e,null);return t?o[t]:o}}function o(e){return'HTML'===e.nodeName?e:e.parentNode e.host}function n(e){if(!e)return document.body;switch(e.nodeName){case'HTML':case'BODY':return e.ownerDocument.body;case'#document':return e.body;}var i=t(e),r=i.overflow,p=i.overflowX,s=i.overflowY;return /(auto scroll)/.test(r+s+p)?e:n(o(e))}function r(e){var o=e&&e.offsetParent,i=o&&o.nodeName;return i&&'BODY'!==i&&'HTML'!==i?-1!=['TD', 'TABLE'].indexOf(o.nodeName)&&'static'===t(o,'position')?r(o):o?e.ownerDocument.documentElement:document.documentElement}function</pre>
----------	--

C:\Users\user\AppData\Local\Temp\~DF4C0C6A7F8B5D7714.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4772217492480291
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9los9lo89lWGl/uCVp+Z+c:kBqolXxGl/J6
MD5:	3AC22A525313CA286F313EC79B8D5FE3
SHA1:	1B7879E92E96D04B5DC4652E8BEBECFDBE32DFEC
SHA-256:	034603AF3236B995E46AEA11D49D7679BBE2A5BC47979E4ADA9926A44CFB0ADE
SHA-512:	62274C5EFFFEAE8B9B9C4FC7F461570807C5A68184D5744BF31B0A5B9D17A996E774D27E159A1CC27F0549FEDE3CAA749E4910BB943FE0503277C6FC57AA09CC49
Malicious:	false
Reputation:	low
Preview:	<pre>.....*%..H..M..{y..+0...(.....*%..H..M..{y..+0...(.....</pre>

C:\Users\user\AppData\Local\Temp\~DF5FAEF6CCA28DFD69.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	35171
Entropy (8bit):	0.46624779608721245
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+FLFFFXF+FKIFKxm3KQmMW8mGWw8m4m+mFmr0b:kBqoxKAuvScS+FLFFFXF+FFFN3HSgb
MD5:	D288185627461842036D36F8BE0318CA
SHA1:	B4407DD8846884C6F3E424AA37BE945F43F595
SHA-256:	EF12273B41FD81C623267A58FA22E3E0650132CF37AEF6CD74A04A79B6723FC9
SHA-512:	1AD8A878B079D0FED73CC0335C8819BCD2C6D59A088AC44A007E0E3D4A8CACE3A03A936CEBFD234ED816137FFADD2525C341D5DA69C1EE2ECA80A3F2CD4F655A
Malicious:	false
Reputation:	low
Preview:	<pre>.....*%..H..M..{y..+0...(.....*%..H..M..{y..+0...(.....</pre>

C:\Users\user\AppData\Local\Temp\~DF726652DFE275AF17.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.6455439471718731
Encrypted:	false
SSDEEP:	48:kBqoxxJhHWSVSEabzMLAovx/5LgYlGpZnZ3jGft2UBup:kBqoxDhHWSVSE+Bvgfg
MD5:	2D3D4A8E41C033E42BB0E8647D626C80
SHA1:	97C10178F581A5561DF93DD57214DA4DDB34B281
SHA-256:	CD8F5BC72E12416D1371B7BF91436B63769EC0C99CB8C01A4505D91A8DDA0411
SHA-512:	DCE4E3ECE67B39401CB2F8D6479ED8373EE9F85350F46C26D928165D257B742C06B94F5AD597EEA7D10CCAA85B85576D3FFFB08D78B5163B7FBEA462E15245F
Malicious:	false
Reputation:	low
Preview:	<pre>.....*%..H..M..{y..+0...(.....*%..H..M..{y..+0...(.....</pre>

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 20:26:29.460459948 CEST	192.168.2.4	8.8.8.8	0x96d7	Standard query (0)	gabriellarodriguezart.com	A (IP address)	IN (0x0001)
Jun 10, 2021 20:26:30.567945004 CEST	192.168.2.4	8.8.8.8	0x6553	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jun 10, 2021 20:26:30.583039045 CEST	192.168.2.4	8.8.8.8	0x6905	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Jun 10, 2021 20:26:30.654016018 CEST	192.168.2.4	8.8.8.8	0xb704	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Jun 10, 2021 20:26:30.876419067 CEST	192.168.2.4	8.8.8.8	0xfc68	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jun 10, 2021 20:26:31.386157990 CEST	192.168.2.4	8.8.8.8	0xbf5	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Jun 10, 2021 20:26:46.217636108 CEST	192.168.2.4	8.8.8.8	0xfe4c	Standard query (0)	gabriellarodriguezart.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 20:26:29.527601004 CEST	8.8.8.8	192.168.2.4	0x96d7	No error (0)	gabriellarodriguezart.com		162.241.114.112	A (IP address)	IN (0x0001)
Jun 10, 2021 20:26:30.617988110 CEST	8.8.8.8	192.168.2.4	0x6553	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 20:26:30.641345978 CEST	8.8.8.8	192.168.2.4	0x6905	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Jun 10, 2021 20:26:30.641345978 CEST	8.8.8.8	192.168.2.4	0x6905	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Jun 10, 2021 20:26:30.716372967 CEST	8.8.8.8	192.168.2.4	0xb704	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 20:26:30.943485022 CEST	8.8.8.8	192.168.2.4	0xfc68	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jun 10, 2021 20:26:30.943485022 CEST	8.8.8.8	192.168.2.4	0xfc68	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jun 10, 2021 20:26:31.452528954 CEST	8.8.8.8	192.168.2.4	0xbf5	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 20:26:46.285185099 CEST	8.8.8.8	192.168.2.4	0xfe4c	No error (0)	gabriellar odriguezart.com		162.241.114.112	A (IP address)	IN (0x0001)

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 20:26:29.883374929 CEST	162.241.114.112	443	192.168.2.4	49740	CN=gabriellarodriguezart.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 Jun 05 23:13:12 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Fri Sep 03 23:13:12 CEST 2021 Mon Sep 15 18:00:00 CEST 2025	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 20:26:29.890131950 CEST	162.241.114.112	443	192.168.2.4	49739	CN=gabriellarodriguezart.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 Jun 05 23:13:12 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Fri Sep 03 23:13:12 CEST 2021 Mon Sep 15 18:00:00 CEST 2025	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 20:26:30.885916948 CEST	104.18.11.207	443	192.168.2.4	49751	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Mar 01 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Tue Mar 01 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jun 10, 2021 20:26:30.895909071 CEST	104.18.11.207	443	192.168.2.4	49750	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Mar 01 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Tue Mar 01 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jun 10, 2021 20:26:31.049500942 CEST	104.16.18.94	443	192.168.2.4	49757	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	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
Jun 10, 2021 20:26:31.051317930 CEST	104.16.18.94	443	192.168.2.4	49756	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	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
Jun 10, 2021 20:26:46.640929937 CEST	162.241.114.112	443	192.168.2.4	49770	CN=gabriellarodriguezart.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 Jun 05 23:13:12 CEST 2021 Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Fri Sep 03 23:13:12 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 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: 6828 Parent PID: 800

General

Start time:	20:26:27
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:	0x7ff648790000
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: 6908 Parent PID: 6828

General

Start time:	20:26:28
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:6828 CREDAT:17410 /prefetch:2
Imagebase:	0x180000
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