ID: 363940
Cookbook: browseurl.jbs
Time: 15:39:34
Date: 05/03/2021
Version: 31.0.0 Emerald

Table of Contents

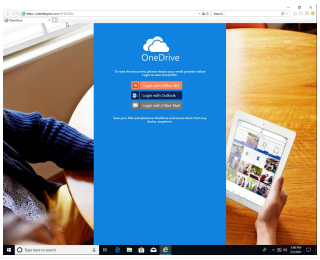
Analysis Report https://plateflippers.com/OH2/GG8/

Overview

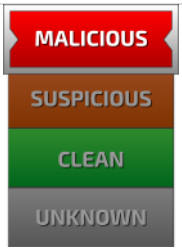
General Information

Sample URL:	http://https://plateflippers.com/OH2/GG8/
Analysis ID:	363940
Infos:	

Most interesting Screenshot:



Detection



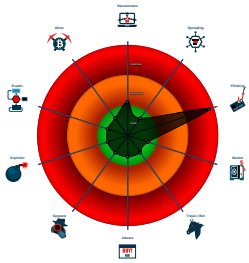
HTMLPhisher

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for subm…
- Phishing site detected (based on sh…
- Yara detected HtmlPhish_7
- Yara detected obfuscated html page
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- Invalid T&C link found
- Yara detected Encrypted html page …

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6904 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6960 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6904 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\2WF3MMUU\GG8[1].htm	JoeSecurity_Obshtml	Yara detected obfuscated html page	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\GG8[1].htm	JoeSecurity_Encryptedhtml	Yara detected Encrypted html page by third party sevices	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
- Multi AV Scanner detection for submitted file

Phishing:

- Phishing site detected (based on shot template match)
- Yara detected HtmlPhish_7
- Yara detected obfuscated html page
- Phishing site detected (based on image similarity)
- Phishing site detected (based on logo template match)

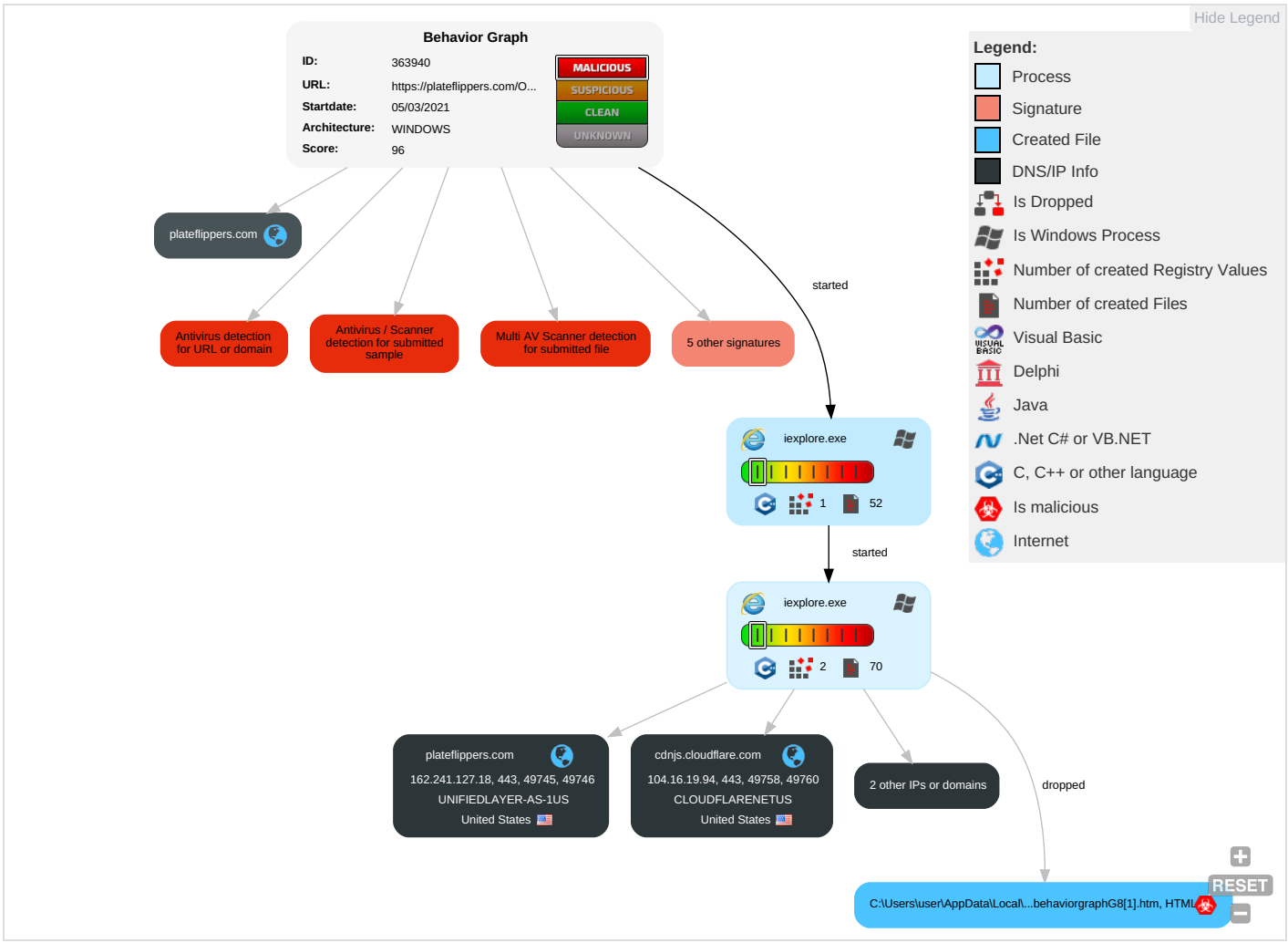
Compliance:

- Uses new MSVCR Dlls
- Uses secure TLS version for HTTPS connections

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impac
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 Partiti
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	Devic Lockc
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	Delet Devic Data

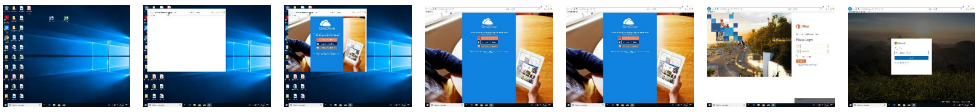
Behavior Graph

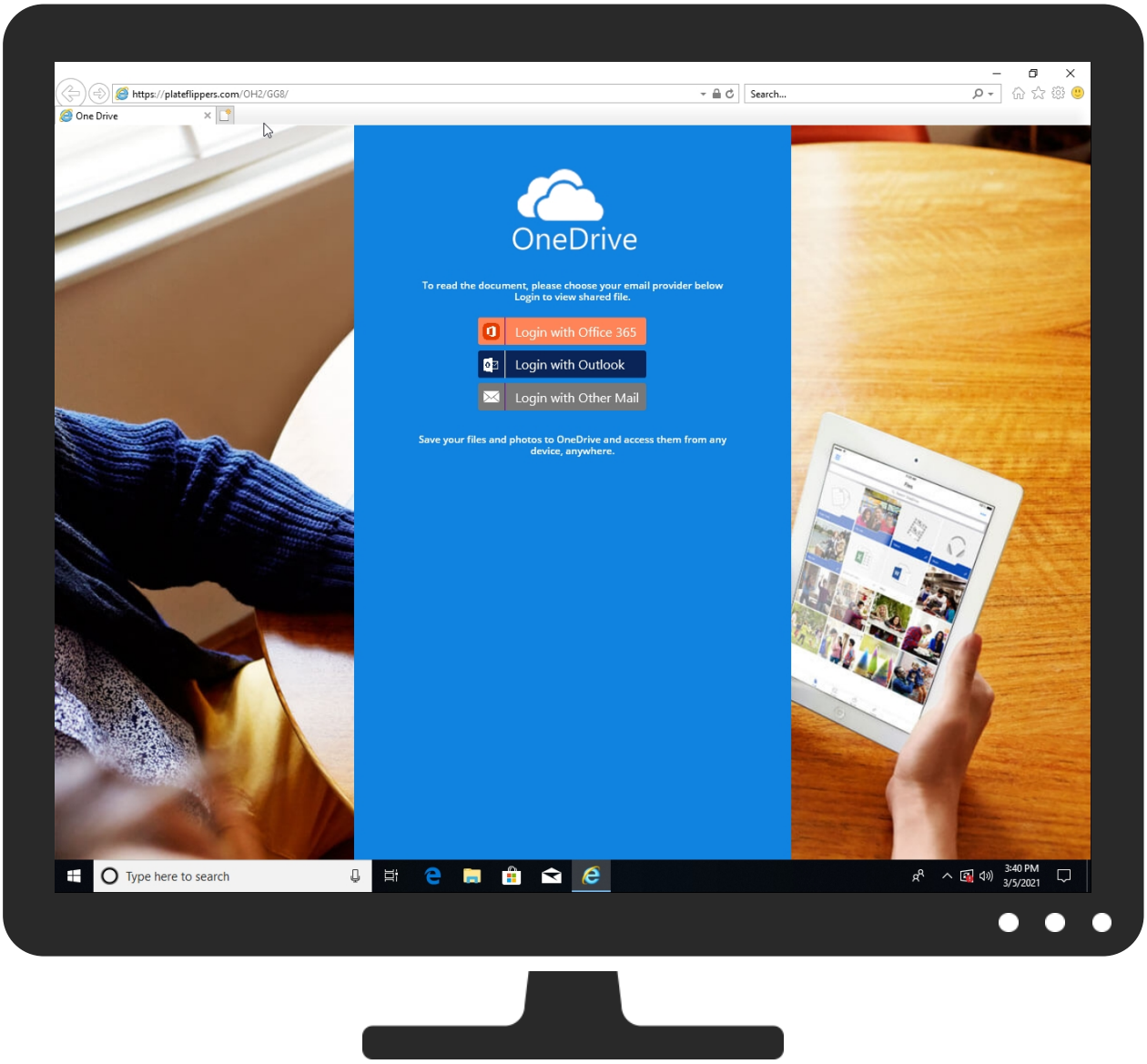


Screenshots

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://plateflippers.com/OH2/GG8/	11%	Virustotal		Browse
http://https://plateflippers.com/OH2/GG8/	100%	Avira URL Cloud	phishing	
http://https://plateflippers.com/OH2/GG8/	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://plateflippers.com/OH2/GG8/Outlook.php	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://plateflippers.com/OH2/GG8/Othermail.php	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://plateflippers.com/OH2/GG8/Office365.php	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://plateflippers.com/OH2/GG8/Root	100%	Avira URL Cloud	phishing	
http://fontawesome.iohttp://fontawesome.iohttp://fontawesome.io/license/http://fontawesome.io/licens	0%	Avira URL Cloud	safe	
http://https://plateflippers.com/OH2/GG8/f	100%	Avira URL Cloud	phishing	
http://https://plateflippers.com/OH2/GG8/Outlook.phpp2/GG8/Office365.php	100%	Avira URL Cloud	phishing	
http://https://plateflippers.com/OH2/GG8/Outlook.phpBSign	100%	Avira URL Cloud	phishing	
http://https://getbootstrap.com)	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
plateflippers.com	162.241.127.18	true	false		unknown
cdnjs.cloudflare.com	104.16.19.94	true	false		high
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
code.jquery.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://plateflippers.com/OH2/GG8/Office365.php	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://plateflippers.com/OH2/GG8/Outlook.php	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://plateflippers.com/OH2/GG8/	true		unknown
http://https://plateflippers.com/OH2/GG8/Othermail.php	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0-alpha.6/css/bootstrap.min.css	Othermail[1].htm.2.dr	false		high
http://fontawesome.io	fontawesome-webfont[1].eot.2.dr, font-awesome.min[1].css.2.dr	false		high
http://https://plateflippers.com/OH2/GG8/Root	{B49B7545-7DC0-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: phishing	unknown
http://fontawesome.iohttp://fontawesome.iohttp://fontawesome.io/license/http://fontawesome.io/licens	fontawesome-webfont[1].eot.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://signup.live.com	Outlook[1].htm.2.dr	false		high
http://https://plateflippers.com/OH2/GG8/f	~DF8ADC395168C1F92B.TMP.1.dr, {B49B7545-7DC0-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: phishing	unknown
http://https://plateflippers.com/OH2/GG8/Outlook.phpp2/GG8/Office365.php	~DF8ADC395168C1F92B.TMP.1.dr	true	• Avira URL Cloud: phishing	unknown
http://https://plateflippers.com/OH2/GG8/Othermail.php	~DF8ADC395168C1F92B.TMP.1.dr	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://fontawesome.io/license	font-awesome.min[1].css.2.dr	false		high
http://https://plateflippers.com/OH2/GG8/Outlook.phpBSign	~DF8ADC395168C1F92B.TMP.1.dr	true	• Avira URL Cloud: phishing	unknown
http://fontawesome.io/license/	fontawesome-webfont[1].eot.2.dr	false		high
http://https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css	Othermail[1].htm.2.dr	false		high
http://https://code.jquery.com/jquery-3.1.1.slim.min.js	Othermail[1].htm.2.dr	false		high
http://https://github.com/twbs/bootstrap/graphs/contributors)	bootstrap.min[1].js.2.dr, bootstrap.min[1].js0.2.dr	false		high
http://https://plateflippers.com/OH2/GG8/	~DF8ADC395168C1F92B.TMP.1.dr	true		unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://cdnjs.cloudflare.com/ajax/libs/tether/1.4.0/js/tether.min.js	Othermail[1].htm.2.dr	false		high
http://https://getbootstrap.com)	bootstrap.min[1].js.2.dr, bootstrap.min[1].css.2.dr, bootstrap.min[1].css0.2.dr	false	• Avira URL Cloud: safe	low
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[1].js.2.dr, bootstrap.min[1].css.2.dr	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0-alpha.6/js/bootstrap.min.js	Othermail[1].htm.2.dr	false		high
http://https://plateflippers.com/OH2/GG8/Office365.php	~DF8ADC395168C1F92B.TMP.1.dr	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://plateflippers.com/OH2/GG8/Outlook.php	~DF8ADC395168C1F92B.TMP.1.dr	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.10.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
162.241.127.18	plateflippers.com	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	363940
Start date:	05.03.2021
Start time:	15:39:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://plateflippers.com/OH2/GG8/

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:	mal96.phis.win@3/42@5/3
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://platefl ippers.com/OH2/GG8/Office365.php • Browsing link: https://platefl ippers.com/OH2/GG8/Outlook.php • Browsing link: https://platefl ippers.com/OH2/GG8/Othermail.php
Warnings:	Show All • Exclude process from analysis (whitelisted): ielowutil.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 52.255.188.83, 104.42.151.234, 104.43.139.144, 88.221.62.148, 13.88.21.125, 209.197.3.24, 172.217.20.234, 172.217.22.195, 13.64.90.137, 40.88.32.150, 51.104.139.180, 152.199.19.161 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, cds.s5x3j6q5.hwcdn.net, fonts.googleapis.com, skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, fonts.gstatic.com, ie9comview.vo.msecnd.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus15.cloudapp.net, skypedataprdcoleus17.cloudapp.net, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, watson.telemetry.microsoft.com, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{B49B7543-7DC0-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8529556903889186
Encrypted:	false
SSDEEP:	192:rCZFZ02fLWOt0ifZNjzMn7BxBDIsfrNajX:r+rj6uJcFnnU
MD5:	961FA85B2766C8D3240EEC0774146A78
SHA1:	97561BA0DEFE39C86AC80C119024C61E9E5CB6BC
SHA-256:	766E5FC530E835D548B2CA6F24E6DE444F0240D7A5B9351024156 62C671900A6
SHA-512:	1BB475AC0AACC0B54682E61C3DFD807009E7ED711B9107806FFA6A166BE26C9DC0FF1BBDEE228FDD3208C32011F3CF59AEA9966AE6F86FFA11F7F706F9AA79CF
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\{B49B7545-7DC0-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	63614
Entropy (8bit):	2.15238594440923
Encrypted:	false
SSDEEP:	384:r7bSeA1SsCSuxkaczAd2J7LmUmLd0FNVTDnIZDs:O
MD5:	7C1C44CB430BD1C5B50D8A2EF81D04CA
SHA1:	685AA0E491E423B7C3CB54A5C6C56B889D454B18
SHA-256:	E4F2A29DC03135ED684BB2D5AC90C5576E3B28AB038176EC58DE629150D45324
SHA-512:	833E700BA2CA307F815DDB8A3BB4076E3AFC7CC7194B8789A91E5134E74B742B96621CF945C59398A20C744D7A012E5AC7E8C0021AD56C2517CF45B3562942E
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\{BAAB9089-7DC0-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.563535857611493

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{BAAB9089-7DC0-11EB-90EB-ECF4BBEA1588}.dat	
Encrypted:	false
SSDEEP:	48:Iw7GcprOGwpa/G4pQ/GrapbShZGQpKjG7HpR/aTGIpG:rhZmQR6DBShzAyT/eA
MD5:	2A3546169B47B2DD6DED7B81CC05A2CC
SHA1:	A5BC81A0AA4809D529C9151840BBAF84C9263488
SHA-256:	CF545D57DDEE32834C667A218639F5B10AA1DA77586AA4FA133C11E769DD6318
SHA-512:	F6EBA2CAF99D96952EEE668CB5BD36935F484108FB6F537A85A23C2C17A954E80FCBCF6099931FCB6715EED4B7D374BC3292C74C36A1C2F69AF75EFA97F6DC4
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\GG8[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	5605
Entropy (8bit):	3.3836916804006383
Encrypted:	false
SSDEEP:	96:pafFagxo1n1IVJDc0HaqqxvP54WXhKRDm:pafFagxo1n1wJDR1UvP54ShKRDm
MD5:	3BB47566F1DB61E9D7C05BA9713CB6AB
SHA1:	098C1CE436BD93F74F4C300C0B793330B587110D
SHA-256:	5A9D4B74A3AC81087E1ED71BF83BE9ECE6CE033C96FEC633C0FDE8ABDAFDAB09
SHA-512:	85A1DD7F9675286CBDCE829A6288AAA06238220FF93CF150DBECDC5D67CB215F7465990300FCB28FA285223CEB71F8424EA0C20EBF7D436337632306286EAF0
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Obshtml, Description: Yara detected obfuscated html page, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\GG8[1].htm, Author: Joe Security • Rule: JoeSecurity_Encryptedhtml, Description: Yara detected Encrypted html page by third party sevices, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\GG8[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://plateflippers.com/OH2/GG8/
Preview:	<script type="text/javascript">.. HTML Encryption provided by www.webtoolhub.com -->.. ..document.write(unescape('%3c%21%44%4f%43%54%59%50%45%20%68%74%6d%6c%3e%0d%0a%3c%68%74%6d%6c%20%6c%61%6e%67%3d%22%65%6e%22%3e%0d%0a%20%20%3c%68%65%61%64%3e%0d%0a%20%20%20%20%3c%21%2d%2d%20%52%65%71%75%69%72%65%64%20%6d%65%74%61%20%74%61%67%73%20%2d%2d%3e%0d%0a%20%20%20%20%3c%6d%65%74%61%20%63%68%61%72%73%65%74%3d%22%75%74%66%2d%38%22%3e%0d%0a%20%20%20%20%3c%6d%65%74%61%20%68%74%74%70%2d%65%71%75%69%76%3d%22%63%6f%6e%74%65%6e%74%2d%74%79%70%65%22%20%63%6f%6e%74%65%6e%74%3d%22%74%65%78%74%2f%68%74%6d%6c%22%20%2f%3e%0d%0a%20%20%20%20%3c%6d%65%74%61%20%6e%61%6d%65%3d%22%76%69%65%77%70%6f%72%74%22%20%63%6f%6e%74%65%6e%74%3d%22%77%69%64%74%68%3d%64%65%76%69%63%65%2d%77%69%64%74%68%2c%20%69%6e%69%74%69%61%6c%2d%73%63%61%6c%65%3d%31%2c%20%73%68%72%69%6e%6b%2d%74%6f%2d%66%69%74%3d%6e%6f%22%3e%0d%0a%20%20%20%20%3c%74%69%74%6c%65%3e%4f%6e%65%20%44%72%69%76%65%3c%2f%74%69%74%6c%65%3e%0d%0a%09%0d%0a%20%20

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Othermail[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	4496
Entropy (8bit):	4.586405882790915
Encrypted:	false
SSDEEP:	48:mvzYDpTKL2pUDa6E1eeLYOOGpbTNmSzRWV1fsuaaG9utBkJgUhq0kekJL:SH0EALYebBrRWV1fsY/L
MD5:	399FBBA751DA034337A211A936B22B22
SHA1:	C1D80614AEAE0E470838974211908 28B3E9043F6
SHA-256:	C7A2BC42652E4C60BFD5F2E4D3A3D8111F1602B3C0C4E04E010D6E32B869645D
SHA-512:	8265B855FF0C4987F19728040CC29F1C01ADAA1EAE4C1B50D255F274BD6CDDE4BCC6C6C27FE16A4B4FFF3E7CD2DC44AA1832B798739178F420302651ABF1139
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://plateflippers.com/OH2/GG8/Othermail.php
Preview:	<!DOCTYPE html>.<html lang="en">. <head>. Required meta tags -->. <meta charset="utf-8">. <meta http-equiv="content-type" content="text/html" />. <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">. <title>One Drive</title>. <link rel="stylesheet" type="text/css" href="css/style.css">. Font Awesome CSS -->. <link rel="stylesheet" type="text/css" href="https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css">. Bootstrap CSS -->. <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0-alpha.6/css/bootstrap.min.css" integrity="sha384-rwoIResjU2yc3z8GV/NPeZWAv56rSmLldC3R/AZzGRnGxQQKnKkoFVhFQhNUwEyJ" crossorigin="anonymous">. jQuery first, then Tether, then Bootstrap JS. -->. <script src="https://code.jquery.com/jquery-3.1.1.slim.min.js" integrity="sha384-A7FZj7v+d/sdmMqp/nOQwliLvUsJfDHW+k9Omg/a/EheAdgtzNs3hpfag6Ed950n" crossorigin="anonymous"></script>. <s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	150996
Entropy (8bit):	5.0354387423773845
Encrypted:	false
SSDEEP:	1536:JGz3B97sTS2k+PwQDEBi8d/g+oomA+iiHML6YVA30UtEMH2UtI:JGP7iA+jML6YVA30UtEMH2UtI
MD5:	7E923AD223E9F33E54D22E50CF2BCCE5
SHA1:	8B7CB193D70BB476DB06651C878DFCD1A7E1C0EE
SHA-256:	AEBF611C1438DC7EC748E9A6364C734066B34BF2A1C7E2FC6511ED784635B50E
SHA-512:	F7652E7FD2A079D9E39F11D51CE7EA1B95C9DD10418ECD386242FF090D61F8094108B5AEA462EFA8BCCA1441F9AEE42CC8F16265DECCC0E4D9B811718A73FE A2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0-alpha.6/css/bootstrap.min.css
Preview:	/*!. * Bootstrap v4.0.0-alpha.6 (https://getbootstrap.com). * Copyright 2011-2017 The Bootstrap Authors. * Copyright 2011-2017 Twitter, Inc.. * Licensed under MIT (https: //github.com/twbs/bootstrap/blob/master/LICENSE). *//*! normalize.css v5.0.0 | MIT License | github.com/necolas/normalize.css */html{font-family:sans-serif;line-height:1. 15;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}body{margin:0}article,aside,footer,header,nav,section{display:block}h1{font-size:2em;margin:.67em 0}f igcaption,figure,main{display:block}figure{margin:1em 40px}hr{-webkit-box-sizing:content-box;box-sizing:content-box;height:0;overflow:visible}pre{font-family:mo nospace,monospace;font-size:1em}a{background-color:transparent;-webkit-text-decoration-skip:objects}a:active,a:hover{outline-width:0}abbr[title]{border-bottom:n one;text-decoration:underline;text-decoration:underline dotted}b,strong{font-weight:inherit}b,strong{font-weight:bolder}code,kbd,samp{font-family:monospace,mono space;font-size:1em}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bootstrap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	48944
Entropy (8bit):	5.272507874206726
Encrypted:	false
SSDEEP:	768:9VG5R15WbHVKZrycEHSYro34CrSLB6WU/6DqBf4l1B:9VIRuo53XiwWTvl1B
MD5:	14D449EB8876FA55E1EF3C2CC52B0C17
SHA1:	A9545831803B1359CFEED47E3B4D6BAE68E40E99
SHA-256:	E7ED36CEEE5450B4243BBC35188AFABDFB4280C7C57597001DE0ED167299B01B
SHA-512:	00D9069B9BD29AD0DAA0503F341D67549CCE28E888E1AFFD1A2A45B64A4C1BC460D81CFC4751857F991F2F4FB3D2572FD97FCA651BA0C2B0255530209B182F2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://plateflippers.com/OH2/GG8/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),requir e("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,n){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function s(t,e,n) {return e&&i(t.prototype,e),n&&i(t,n),t}function r(){return(r=Object.assign||function(t){for(var e=1;e<arguments.length;e++){var n=arguments[e];for(var i in n)Object.pro totype.hasOwnProperty.call(n,i)&&(t[i]=n[i])}return t}).apply(this,arguments)}e=e&&e.hasOwnProperty("default")?e.default:e,n=n&&n.hasOwnProp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1887
Entropy (8bit):	5.187998229445049
Encrypted:	false
SSDEEP:	48:SY3QW9Y3QLZY3QxTGY3QC7Y3Qw6QOWGOLpOxTvOChOw6b:SYgW9YgLZYgxTGYgC7Ygw6QOWGOLpOxo
MD5:	7AD11B51C8A9918ADE502DA9DE063EFF
SHA1:	ABF598711588628073EE60E294F288AB76EA187A
SHA-256:	5A270BD50EF12A93ABAE711C806D6C59D58B0E0D2A9B3463A8268DC3D2EA6857
SHA-512:	6932EACAB01B2443439A31537BC694BB6F611473BE6FC702DBCA92BC2DE27736F2A363744F14CCCDE7C05E660ACCADDA66523E5068371EFBDD8551B2375458 A
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKWyV 9hrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/opensans/v18/mem6 YaGs126MiZpBA-UFUK0Zdcs.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 600;. src: url(https://fonts.gstatic.com/s/ opensans/v18/memnYaGs126MiZpBA-UFUKXGUdhrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 700;. src: url(https:/ /fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKWiUNhrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 800;. src: url(https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKW-U9hrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\font-awesome.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	31000
Entropy (8bit):	4.746143404849733
Encrypted:	false
SSDEEP:	384:wHu5yWeTUKW+KlkJ5de2UYDyVfwYUas2l8yQ/8dwmaU8G:wwlr+Klk3Yi+fwYUf2l8yQ/e9vf
MD5:	269550530CC127B6AA5A35925A7DE6CE
SHA1:	512C7D79033E3028A9BE61B540CF1A6870C896F8
SHA-256:	799AEB25CC0373FDEE0E1B1DB7AD6C2F6A0E058DFADAA3379689F583213190BD
SHA-512:	49F4E24E55FA924FAA8AD7DEBE5FFB2E26D439E25696DF6B6F20E7F766B50EA58EC3DBD61B6305A1ACACD2C80E6E659ACCEE4140F885B9C9E71008E9001FBF4B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css
Preview:	/*!. * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */@font-face{font-family:'FontAwesome';src:url('../fonts/fontawesome-webfont.eot?v=4.7.0');src:url('../fonts/fontawesome-webfont.eot?#iefix&v=4.7.0') format('embedded-opentype'),url('../fonts/fontawesome-webfont.woff2?v=4.7.0') format('woff2'),url('../fonts/fontawesome-webfont.woff?v=4.7.0') format('woff'),url('../fonts/fontawesome-webfont.ttf?v=4.7.0') format('truetype'),url('../fonts/fontawesome-webfont.svg?v=4.7.0#fontawesomeregular') format('svg');font-weight:normal;font-style:normal}.fa{display:inline-block;font:normal normal normal 14px/1 FontAwesome;font-size:inherit;text-rendering:auto;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.fa-lg{font-size:1.33333333em;line-height:.75em;vertical-align:-15%}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-fw{width:1.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\fontawesome-webfont[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), FontAwesome family
Category:	downloaded
Size (bytes):	165742
Entropy (8bit):	6.705073372195656
Encrypted:	false
SSDEEP:	3072:qbhEnD+IzsU9z9QJ6/P3Xe2iEiEPGFCMW1JVJG6wVTDsk6BmG6S1yKshojskO+b2:qenD+IzsU9z9QJ6/PO2FiEP2C/DVJG6I
MD5:	674F50D287A8C48DC19BA404D20FE713
SHA1:	D980C2CE873DC43AF460D4D572D441304499F400
SHA-256:	7BFCAB6DB99D5CFBF1705CA0536DDC78585432CC5FA41BBD7AD0F009033B2979
SHA-512:	C160D3D77E67EFF986043461693B2A831E1175F579490D7F0B411005EA81BD4F5850FF534F6721B727C002973F3F9027EA960FAC4317D37DB1D4CB53EC9D343A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/fonts/fontawesome-webfont.eot?
Preview:	n.....LP.....Yx.....F.o.n.t.A.w.e.s.o.m.e.....R.e.g.u.l.a.r...$.V.e.r.s.i.o.n. .4...7...0. .2.0.1.6.....F.o.n.t.A.w.e.s.o.m.e.....PFFTMk.G.....GDEF.....p... OS/2.2z@...X...`cmap..:.....gasp.....h....glyf...M.....L.head...-.....6hhea.....$hmtxEy.....loca...\.....maxp.,.....8... name....gh....post.....k....u.....xY_.<.....3.2.....3.2.....'.....@.....i.....3.....3...s.....pyrs.@. ....p.....U.....].....y...n.....2.....@.....z.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\mail[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 100 x 87, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1106
Entropy (8bit):	7.176105528957688
Encrypted:	false
SSDEEP:	24:rTtaBegujKwSx2UKzpZtPcCdBR1uj7cxRqnwFT2C4z2MlNvM2NOYVrng:rTtWSwxKzpZvoExQwFJfKiyOYVLg
MD5:	D9F81CF593394338BD133AA77B0ECBAF
SHA1:	24AB26A812E74CBB08BB17E495F8852A3DF5A038
SHA-256:	2EBC65A696544B8D69ADE5F136250A9548D4BADF1B9AD459E63FF68E7A985C69
SHA-512:	28370A1CE7F1F3CA386187DF2FBADAE154E151DE5794913FD0DAE42B26545BE39E9A6E2C855F4EB3D267210768FF7AE7D15268C3BEDA53D88FE9AA878ECF065
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://plateflippers.com/OH2/GG8/images/mail.png
Preview:	.PNG.....IHDR...d...W.....e....PLTE.....wy....4tRNS.9.....j...0!.....A.I<4.\.bN,'...|nfXFu.V.R6xs.....IDATh...r.@.E.k3c..(j...D3....[..P....b..K.L.....2..b...;@1./...C9....s..w..d..P.9.....e..''..E3..A:;P.sf2..../..b.,..Z/Sd$..[..>@c...Jo:DF...<..h6N.c.....'wr%..\|..Z6.%....Gm...9pW.I?.'.Q.0.?....:..^G-.}.....TE...2.\|.?..2..!.Q....c..*!....R.9....*0c...xR..5.]V.$._.x^..t'..o.....;|<.rF...bE..'...F..$.m;.%h;v.!PC.....!.C..F=.t9\|....!.\.....^..^_.\|.....H...1..*_'!o*..g...!.2.&.K.F=.0....(Dc...-.L'..@.d.O..6nh....[..YJ.....\.nTH,.....qA\n.w.}..Dp.8E....OV..&.{..I..mi[..)0.K.....;M$.."C.O..h....l..C}.....c'.h.....+....T...e2_kI..5^z.....U...nv.r.t.t.....U%....h[...M.RM.a.n}...y.n.$....T`$.[{V2K.V.6.lgOH..C...N..L.^.^tTF.....%..I..>.?..H4...@-....#./C>Bm.@..}I..D....=.....o

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\mem5YaGs126MiZpBA-UN_r8OUuhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18668, version 1.1
Category:	downloaded
Size (bytes):	18668
Entropy (8bit):	7.969106009002288
Encrypted:	false
SSDEEP:	384:Wv4QHZChiRh3lwLOf8cWN78NXpcr6gBUA9CD/q4cOPZmPO:WvwhNOkvvxC7qnc
MD5:	A7622F60C56DDD5301549A786B54E6E6
SHA1:	D55574524345932DB3968C675E1AEA08C68A456F
SHA-256:	6E8A28A0638C920E5B76177E5F03BA94FCDEDD3E3ECD347C333D82876B51C9C0
SHA-512:	1A842E5EDFFFFBAE353AD16545D9886E3E176755F22B86ECCC9B8B010FC79DB7194B7C5518CC190BF5B78B332C7D542B70A6A53B3BAF23366708DF348C2C2D9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN_r8OUuhv.woff
Preview:	wOFF.....H.....n0.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....^...`}...cmap...`.....X..cvt .....]....fpgm...t.....~a..gasp.....#glyf... ..8...WP..M.head..@....6...6..F.hhea..A.....$...chmtx..A8....._{loca..CL.....K.4&maxp..E.... .. ....name..E0....."c?Jpost..F.....x.U..prep..G.....:..]..... .....x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`fig.a`e``..j...(.../2.1..`b.ffcfeabbi``Pg``..b.. 0t.vfp`P...M...C.G/S....\...=.6 .....m/....x.\.!..q.....#aff... #1Q@.'U..@5.".llt.Aa#.f\c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$K..$..`.g.e..... ..... R.g.....?.....x.)d.....$...."....0.#.A@X..0.....x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...s.3.S...co..o.~.Zy.u...kW.\.t...N

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\memnYaGs126MiZpBA-UFUKW-U9hrIqU[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17788, version 1.1
Category:	downloaded
Size (bytes):	17788
Entropy (8bit):	7.967181593577758
Encrypted:	false
SSDEEP:	384:Vp3UxvLq7eMDKdiXVYFbQk9YlD/XmhJGSiQ3L+CEW/9fE+QH:jgjq7ejOQMUeD/AGO6CB/98+QH
MD5:	92DA6F116D973BD334CF9B3AFDB29C4F
SHA1:	C7E59C92F4D8391276FB0A3A55528CF3965478E7
SHA-256:	49B6274BCCB5C6B31E20CEBB213D96197B522B1FB9C95B8649A0626EDB5BD9D8
SHA-512:	B3483F5137EAE074BDC95262B8C5D6049C4E7AF276F3EB1DDC3097ED3FBFB2C43110341B78E0B388E6B9B5D186168CD86DA324496CB08F909C60FEBFB3E2079
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKW-U9hrIqU.woff
Preview:	wOFF.....E\.....f.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....]...`....cmap...`.....X..cvt .....o.....fpgm.....s.ugasp...(.....#glyf...8 ..4...N.-.W.head..=0...6...6....hhea..=h..."...$....hmtx..=....8.....|&.loca..?.....P..maxp..A.... .. ....name..A.....8Gtpost..B.....x.I..prep..D`.....@..R..... .x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.%..@0...?.%.N.O:Zg..TjL...Bk..-.a ..5.j.F...`...^..3.V.P..P.4..c....[..]..9.... ..T(.q...x.\.!..q.....#aff...#1Q@.' U..@5.".llt.Aa#.f\c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$KY...e@.,..".9....x.....3.....e.. =L.....`.Q..1.Q.....uF.F[F}Fe.....-.p..... ..x.TGw.F.....)..)7.W..`*.j.-...=*'_..sI...2...O>....[tt....TK]..|...G.....^.m..=..x

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Onedrive-logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 170 x 114, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	4423
Entropy (8bit):	7.924731439527259
Encrypted:	false
SSDEEP:	96:hYNgH0x07J2QQZHs6JKaDsZV3ZN/C+5bGUR3vUcmt1B3:INQEHx5Dcbal1d
MD5:	FFC68AE7FD5A2D7A7CEC7185717B6E88
SHA1:	ABBCEBC2E0794C8F30DF0035881D4405D3A1D69B
SHA-256:	4603EA1B2F9DF0C9D4F2A253C550FFBAF27EA2CB53ECDE4277B2ACF9DDE33979
SHA-512:	F90CABBC9E1F2A1F8386C9C6C51729FC6678D35EAD9C0B7C02D50E5413BA88F5BE0B45327761B0C4617D8D2A2109EEF887A1F486F919BF554A6089AF8ED5C236
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://plateflippers.com/OH2/GG8/images/Onedrive-logo.png
Preview:	.PNG.....IHDR.....r.....PLTE..... ....+.....tRNS.....8.....=.UP0&..~!...hW+....J.u.....vkZ...dL?.....`[F.....C3..... .....mk["'.....pT.....|?!.....|m-.....WTPHB;94.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Outlook[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Outlook[1].htm	
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	9075
Entropy (8bit):	5.166359155420789
Encrypted:	false
SSDEEP:	96:RL9O4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDmnhGzoxLrPPDlcOyeBLYYnNdt72tR:x9ToSBjlevudl9nKwMxzNYYN/mma
MD5:	41533DAD7B078D172234686E36B80E5B
SHA1:	695F0E1AE148DC62106C2044C362DEBCEED2F4C9
SHA-256:	6353840890F462A1DE1A412650A42F45E935071015B837C1D703C0BBAAFED53C
SHA-512:	D31D54559490C6B16ABA5477029F85D4EE7F4002404DE44201D4810A809E8697D2729470517630A66969917132BA84BFE2F1E1E75EEFAA335EA7DAE77574E7A0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://plateflippers.com/OH2/GG8/Outlook.php
Preview:	<!DOCTYPE html>.<html lang="en">. <head>. Required meta tags -->. <meta charset="utf-8">. <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">. <title>Sign in to your Microsoft account</title>.... <link rel="stylesheet" href="css/bootstrap.min.css">. Font Awesome CSS -->. <link rel="stylesheet" type="text/css" href="https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css">. Bootstrap CSS -->. <link rel="stylesheet" type="text/css" href="css/style.css">..</head>.<body>. .. . .<div clas s="inner">. . . .<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M 44.836,4.6V18.4h-2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\jquery-3.1.1.slim.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	69309
Entropy (8bit):	5.3700159283175415
Encrypted:	false
SSDEEP:	1536:dNhEyjjTikEJO4edXXe9J578go6MWXqcVhzLyB4Lw13sh2bTQKmPNsvDU8Cur:Dxcq0hzLZwpsYbIyvDU8Cur
MD5:	550DDFE84A114F79A767C087DF97F3BC
SHA1:	310BD0C04196573315C2E8446776685AC2961724
SHA-256:	FD222B36ABFC87A406283B8DA0B180E22ADEB7E9327AC0A41C6CD5514574B217
SHA-512:	B6A9146FFE380A32C89D48BAF900DD5E346B0D603B8AFCFAD070970E56BDC744E8A8B053C2EF8A3107F4A3C2BDD11EE470E05557F542FFEDE5FF54468EE186C4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.1.1.slim.min.js
Preview:	/*! jQuery v3.1.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_evalUrl,-event/ajax,-effects,-effects/animatedSelector,-effects/Tween,-deprecated	(c) jQuery Foundation	jquery.org/license */.!function(a,b){"use strict";"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)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.1.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_evalUrl,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\mem5YaGs126MiZpBA-UN7rgOUuhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18900, version 1.1
Category:	downloaded
Size (bytes):	18900
Entropy (8bit):	7.96514104643824
Encrypted:	false
SSDEEP:	384:nejx4dDcsFhu/3v79dEAUdH6XSw1fz9fKQm9LQNG/X1epB:ejadDrhYTf3Udaieza98Nbz
MD5:	1F85E92D8FF443980BC0F83AD7B23B60
SHA1:	EE8642C4FAE325BB460EC29C0C2C9AD8A4C7817D
SHA-256:	EA20E5DB3BA915C503173FAE268445FC2745FC9A5DCE2F58D47F5A355E1CDB18
SHA-512:	F34099C30F35F782C8BB2B92D7F44549013D90E9EEDE13816D4C7380147D5B2C8373CC4D858CDF3248AAA8A73948350340EE57DAE9734038FC80615848C7133E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN7rgOUuhv.woff
Preview:	wOFF.....l.....p.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....^...`....cmap...`.....X..cvt .....]....-...fpgm...t.....s.ugasp.....glyf...$ ..9...Y..(.head..A....6...6.%l.hhea..B,.....$.)..hmtx..BL.....O,loca..D`.....9yfmaxp..F$... ... .q..name..FD.....#.>.post..G4.....x.U..prep..H.....k..... .....x...5.A.....m."gW..`.L..&N".?.....lF....a.^...b1.....Uh."4...>..=x.c`f.g.....:....Q.B3_dHc.....@`...../..?....^..... 9.8.m@J....w..!..x.\.!..q.....#aff...#1Q@ .'U..@5.".llt.Aa#.f\c.W....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:....F....GG.g.s,x.>0....v..l;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g``..$KY...e@.,q@.j...o@<..O.H.t..... .....c .p@.....3lbd.....-.}.M...!...!....x.TGw.F.....)..)7.W..`*.j.-...=*_..sI...2...O>....[tt....TK]..|...G.....^.m..=..x.q...+./].p...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\mem5YaGs126MiZpBA-UN8rsOUuhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\mem5YaGs126MiZpBA-UN8rsOUuhv[1].woff	
File Type:	Web Open Font Format, TrueType, length 19072, version 1.1
Category:	downloaded
Size (bytes):	19072
Entropy (8bit):	7.966673384993769
Encrypted:	false
SSDEEP:	384:UCwUC2nJxPRk+P/Qvm6DBM1W71wcdDmyBE+2fweE9m0aGuTeopiH:PJC2nJxP++P/36QWpwNyb2tqgk
MD5:	05EBDBE10796850F045FCD484F35788D
SHA1:	07744CFE76B8C37096443A6BCC3FBD04F93AD05B
SHA-256:	35EB714D45479FE35586513C7D372CED0AE3E26EB05883950BEA2669C6E802AA
SHA-512:	D4F293115640C05E3134D635AA077BC91BF35E80463C93C14646D97784CD9FC8D4CD4E10EEAA7BE621DBD9FA0DE5BE943328014ED505C217E61769F76BFA7F4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN8rsOUuhv.woff
Preview:	wOFF.....J.....p.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....^...`...vcmap...`.....X..cvt .....g.....o.[fpgm...|.....s.ugasp... .....#glyf...0 ...".Yr....head..BT...6...6....hhea..B.....$....hmtx..B....*....#.C.loca..D.....n..maxp..F.... ... .name..F.....%.@cpost..G.....x.U..prep..Ip.....1..S..... x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`f.cV``e``..j...(.../2.11s01qs.1s.01.400.300x.....:.;380(...&.O.....)B..q>H.%.u..R``.....x.\.!..q..... .#aff...#1Q@.'U..@5.".llt.Aa#.f|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g``..$K..(..`.e.a.a`....C ..L..@t.....A..L..&.....1\gta.e....320.0...2.g.j...=...x.TGw.F.....)..)7.W..`*.j.-...=*'_..sI...2...O>....[tt....TK]..|...G.....^.m..=..x.q...+.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\mem5YaGs126MiZpBA-UNirkOUuhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18696, version 1.1
Category:	downloaded
Size (bytes):	18696
Entropy (8bit):	7.96597476007567
Encrypted:	false
SSDEEP:	384:yeQHZsdOZKOlVrf0uvAxZEw5w7Yc3XGi/L6:dBbVwuvAYYw7THc
MD5:	449D681CD6006390E1BEE3C3A660430B
SHA1:	2A9777AFC07BF0BB4BB48F233ED7C4BCBDB60760
SHA-256:	57C79375B1419EE1D984F443CDA77C04B9B38C0BE5330B2D41D65103115FFD72
SHA-512:	8B8436670BB4D742AFA60ABA29D7A78F3788CBEF9353C2896AA492618CF1B22E9A0679972AB930E2F2D4732F3B979C023D25AA0FA86C813AC674524FD4ECA2BE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UNirkOUuhv.woff
Preview:	wOFF.....I.....m.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....^...`.-..cmap...`.....X..cvt .....[.....4fpgm...p.....~a..gasp.....glyf... ...8...W.J.4.head..A....6...6...Mhhea..A<.....$...#hmtx..A\... .....IT.loca..C|.....6..umaxp..E@... ... .t..name..E`.....#.@Ppost..FP.....x.U..prep..H.....x..n..... .....x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`fy.....:....Q.B3_dHc.....@`...../..?....^..... 9. .m@J.....x.\.!..q.....#aff... #1Q@.'U..@5.".llt.Aa#.f|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$KY...e@..,A.".m....x.....3 .....?.[.o...2...:...a..b.)@.Y.....v1.b4d...36 ..x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...s.3.S...co..o.~.Zy.u...kW.\.t...N.KG.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\mem8YaGs126MiZpBA-UFVZ0d[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18100, version 1.1
Category:	downloaded
Size (bytes):	18100
Entropy (8bit):	7.962027637722169
Encrypted:	false
SSDEEP:	384:aHQHZuiZQFFlimUy1oml4hN2Vmw1Qa57YC74ObDDj08X0UJQiXc:1ZQT0UySml4bEmAP5EC7PbDH4U1M
MD5:	DE0869E324680C99EFA1250515B4B41C
SHA1:	8033A128504F11145EA791E481E3CF79DCD290E2
SHA-256:	81F0EC27796225EA29F9F1C7B74F083EDCD7BC97A09D5FC4E8D03C0134E62445
SHA-512:	CD616DB99B91C6CBF427969F715197D54287BAFA60C3B58B93FF7837C21A6AAC1A984451AEEB9E07FD5B1B0EC465FE020ACBE1BFF8320E1628E970DDF37B0F0E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem8YaGs126MiZpBA-UFVZ0d.woff
Preview:	wOFF.....F.....i.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....^...`~]..cmap...`.....X..cvt .....Y.....M..fpgm...p.....~a..gasp.....#glyf... ...6...S...]head..>....6...6..cphhea..>.....$....hmtx..?.....[$loca..A4.....f..maxp..B.... ... .name..C.....&:A.post..D.....x.U..prep..E.....C..... ..x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`f..8.....u..1...<.f.....A.....5....1...A._6..".-..L.....Ar,.....3..(....x.\.!..q.....#aff...#1Q@.'U..@5." .llt.Aa#.f|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$KY...e@.,.."..... .....?....%.g....Z..... ("..o..Y..Bu342.e.....0.....M=.....x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...s.3.S...co..o.~.Zy.u...kW.\.t...N.KG.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\tether.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\tether.min[1].js	
Category:	downloaded
Size (bytes):	24989
Entropy (8bit):	5.18502272346698
Encrypted:	false
SSDEEP:	768:1Jc67wdFbgDo6h+T7zMczQvoK/ww8l31g9CZQ5nAgM:zn74bsopz+AK/wM5Af
MD5:	ECDFD3DC464CEDA5F483BB5C96A6E3D2
SHA1:	CBDD0A2B2DD7A9CFC5DB3F33E34323AFA0CA55A3
SHA-256:	80BD626EB6D57112072A508EE4E5CE3C2FE5673FE0A5D029810033B24AAA5E9F
SHA-512:	1EC6758BDBE5A34D656DA7BE28897FFFA28FC6438EEB148F2363DE7EC6620BC2E6496F4A0D63182BD8E136A13D5EC6E31B2AE740067AB121EFB67475DAC24F8C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/tether/1.4.0/js/tether.min.js
Preview:	!function(t,e){"function"==typeof define&&define.amd?define(e):"object"==typeof exports?module.exports=e(require,exports,module):t.Tether=e()}(this,function(t,e,o){"use strict";function i(t,e){if(!(t instanceof e))throw new TypeError("Cannot call a class as a function")}function n(t){var e=t.getBoundingClientRect(),o={};for(var i in e)o[i]=e[i];if(t.ownerDocument!==document){var r=t.ownerDocument.defaultView.frameElement;if(r){var s=n(r);o.top+=s.top,o.bottom+=s.top,o.left+=s.left,o.right+=s.left}}return o}function r(t){var e=getComputedStyle(t)||{},o=e.position,i=[];if("fixed"===o)return[t];for(var n=t;(n=n.parentNode)&&n&&1===n.nodeType;){var r=void 0;try{r=getComputedStyle(n)}catch(s){}if("undefined"==typeof r||null===r)return i.push(n),i;var a=r,f=a.overflow,l=a.overflowX,h=a.overflowY;/(auto|scroll)/.test(f+h+l)&&("absolute"!==o||["relative","absolute","fixed"].indexOf(r.position)>=0)&&i.push(n)}return i.push(t.ownerDocument.body),t.ownerDocument!==document&&i.push(t.ownerDocument

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\Office365[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	5495
Entropy (8bit):	4.462568215272766
Encrypted:	false
SSDEEP:	48:mvzmTKL2pUDGKcbDiHjzafvnMuaQtxPyatjEhLHMczSH2d4yUz6E1eeLYOOGpbTj:Sx0ED+fvnMYtxaat+LHXzSHPyU3LYebn
MD5:	E52D762B4E73E5F5924D5CC544B1E765
SHA1:	1248AC98038C71D032ED1AB2105BB133B6846B3D
SHA-256:	399C3592FBFF1A1C12B4C97DC1F6720E1A3316FF33FBFA069BD7CF0FFF40E606
SHA-512:	A01BCF9FF279AA7E9390AA1BDD07E0BC3817B1E901FE96F899E59EEA1A2192B705273CA9A4C8864035FDDFA4273D1E69489BC4B20219F8FD7092468147CC7EC3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://plateflippers.com/OH2/GG8/Office365.php
Preview:	<!DOCTYPE html>.<html lang="en">. <head>. Required meta tags -->. <meta charset="utf-8">. <meta http-equiv="content-type" content="text/html" />. <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">. <title>One Drive</title>.. Font Awesome CSS -->. <link rel="stylesheet" type="text/css" href="https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css">. Bootstrap CSS -->. <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0-alpha.6/css/bootstrap.min.css" integrity="sha384-rwoIResjU2yc3z8GV/NPeZWAv56rSmLldC3R/AZzGRnGxQQKnKkoFVhFQhNUwEyJ" crossorigin="anonymous">. <link rel="stylesheet" type="text/css" href="css/style.css">..</head>.<body>.. . . . <img class="img-fluid ofc" src="images/officebg.jpg" alt="Office">. . <div class="col-md-4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	3774
Entropy (8bit):	5.187998229445049
Encrypted:	false
SSDEEP:	96:SYgW9YgLZYgxTGYgC7Ygw6QOWGOLpOxTvOChOw6GYgW9YgLZYgxTGYgC7Ygw6QOI:Hl6k+2TpEIszezoTl6k+2TpEIszezob
MD5:	92404C8DCB1F1863E5ADCA427FF6E876
SHA1:	592107E0DF7ADFC6C7D5063E2B41B86F449E48D1
SHA-256:	CFF86CE07328574D51AAE24D05AEA68B4587B0B2D75E8FCB985347771E2DCB5D
SHA-512:	7DE5A3B443C21E78F7BE81DD98BE5845311F7230E9435C6BDA99F7C96A97F867FEC853F4177C1B46C45D3D005CDC30217E0D25AAB0203B03879C9E8DA46DB8C
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKWyV9hrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/opensans/v18/mem6YaGs126MiZpBA-UFUK0Zdcs.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 600;. src: url(https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKXGUdhrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKWiUNhrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 800;. src: url(https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKW-U9hrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\landing-devices-bg[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\landing-devices-bg[1].jpg

File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1200x800, frames 3
Category:	downloaded
Size (bytes):	160872
Entropy (8bit):	7.983227926427131
Encrypted:	false
SSDEEP:	3072:2uSUXBjNQkwlonMsi5EixPv7LxYLHV0zXIHTQaihnyga+:2dUXN4lqLixPv7t2QXCQaid9
MD5:	55174EA1C3DF4966ED13D25A6223999D
SHA1:	FA1E418627CE2C16FF594A9615B1D53E5F676FFF
SHA-256:	C86C4A6731077F1994A8CAECCB1FC06477EA35A5B6ABBB4ABDE1D06B8EF9FF32
SHA-512:	BD5FB38C3BBCCD3F9C7E9E21DE86CD5C1846CF54406FB999649D76CD92D98214585BF00554FE44AE63B97EC9E30252D36CEDD39459A365ECF54E110911D8CE AD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://plateflippers.com/OH2/GG8/images/landing-devices-bg.jpg

Preview:

......JFIF.............C....................................!*$..(..%2%(,-/0/.#484.7*./....C... ....
..=... @..... ....'.W].8 @........ ....hS....A J.....s.....2j.l.!m..C..M& ...8..0.8... p`@..!.....;.......5..$0..!0.a"g#.UN.3.NT.D.L.D.sz.OO.y..D..b(.g!.|...o.9.8.WK..\....LK..@i.Y...N.M
..56.mR./`.@...A..A.......(9...;,@......RET.n".....F....BT.8.Wf$_?...oAVd...M...`!...H.46...4...80 d8& d pL`HA..U...p.'?..$C... .....C.i...D......G/.S..../..M.D.is..3.5..0..5b...y.C.t.Z...."
.n5....m\..sb...B.................*.75.-.Q.....PEA..D.....e....@.r ..l.O..LLv..\.Y.U..F.....4...l..6.6........&$ @........=w....>../...j...17c;..^..|..l...(.....4..L6N...+:r.yW..Y..u\.N\.O2T....8^;.~
..g..f.x.x...}.=.....qj..V)['.l........... @......V.L.....l...@(....R... N9.@.!Y.q|..d.)..y.q....)...h..l..&.a.0.h... @.....@...!......../

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\memnYaGs126MiZpBA-UFUKWiUNhrIqU[1].woff

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17452, version 1.1
Category:	downloaded
Size (bytes):	17452
Entropy (8bit):	7.960788191365059
Encrypted:	false
SSDEEP:	384:gVRT8VGShcBuPgTnSzgEuY86rgt710WmLonjMKsZMQAZ:s3ShcBuASzgEuYPNn0nDRQAZ
MD5:	BF72679CA22E53320BEAEA090E8BB07D
SHA1:	F3BAA33E986EC10D6F0C8211A826242441D52CC7
SHA-256:	1E742589D91A4B7E3888284A43A73675F312D3D6C4E78B3B76EBC36292646100
SHA-512:	F8FFC70E2E187EFBC785A52959BB26F605FEFB904D27B73EA4E1012DCC35569A78144751F761AA30D7B4AB0E5951B91322EA322BAF792C18E359C2ED79BBAF6 E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKWiUNhrIqU.woff

Preview:

wOFF......D,......eT........................GDEF................GPOS................GSUB.......X...t...OS/2.......]...`....cmap...`.........X..cvt ....b.....g.ifpgm...x........s.ugasp................glyf...(
..3...NH7X..head..<....6...6..{.hhea..<T..."...$...ahmtx..<x...).....>/Sloca..>............maxp..@l... ... .x..name..@.........)/C.post..A........x.I..prep..C<...
x...5.A......m."gW..`.L..&N".?.......IF....a.^...b1.................Uh."4...>..=x.c`f9......u..1...<.f.......................b.. 0t.vfPdP...M...C.G/S....|..K..6 .....t......x.\.!..q......#aff...#1Q@
.'U..@5.".llt.Aa#.f|c.W.....'..X..!..C...ITPE.;..V.j......0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e(}.IS2..uc]p.........M.x.c.a.g.c..$KY...e@.,q........x........3...
........%..=.d.......#..6.e..L@6.3.e.....1._....#...x.TGw.F........)..)7.W..`*.j.-...=*'_..sI...2...O>....[tt....TK]..|...G.............^.m..=..x.q...+./].p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\microbg[1].jpg

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, 1920x1080, frames 3
Category:	downloaded
Size (bytes):	259416
Entropy (8bit):	7.9781594411712575
Encrypted:	false
SSDEEP:	6144:fCbqQ5UnngLOssLz8NL7c9Iw9uQdsAPJWN:foZqnnIIv8NHc9Iw9ugZi
MD5:	C58B50331BCDD1C2B4FFB5E7A456E08A
SHA1:	2D4E7108635F07451A2578D9F847BDC4023F279D
SHA-256:	2777ABE0312E6B49428D5D7F7F42E43AF620793F86F823F2E045968AFBDDDB63
SHA-512:	BC269C47452E49097C1CF91EA527408234263C7039FAEA08EE57F80E53FC6F813737C07FFF0731D40AB1AE2A9AFCACC1E1433F4A0C8A36F3860DC32FF42ED6A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://plateflippers.com/OH2/GG8/images/microbg.jpg

Preview:

......JFIF.............C....................................%...#... , #&')*)..-0-(0%()(...C...........(...(((......8..
.............$_..H..0.$ FH.....@`.....2P.....$Hc..T..TB.d1.. ..$.'.1.......V0....@..v...B.J........$.......@..Y.. .",.U$.T.!.@+.B..... .q...........@ ....(..U@...*"P@.@......J.L.6.@.0....D..
....D1....h..P.1..D...Y....T..@.`.I...C....1.#..`1.d....(.+............f........@ ..,...A3.6%..%..!...(B.... ..@ .....B....@ .....V..."...J.$.@....$N$. ..0.&D........%(!....p.B....I1.!..H-.H.*.!$@@..
.............0......v....(..N..+.'h9........ ...#... ..V..X.....Q..!..V(@!..A..@ . ..@...H.. ....$.h!."...@%d@..........2$.., ...`0Y..+..`..2J..!.....dU.T..c..d..A`.5......:..).:...t+..j.B@...........
.L..$A.E .B...l.....$@ .P..)....B.......... ....D.*.....B.....f.Q..D..1.....2DR 0....0...8T....5c..bFJ.+..cY.0.C...B.BG.]9ZJ...j!.`0..Pp.0........ ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\microsoftlogo[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 115 x 26, 8-bit colormap, non-interlaced

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\microsoftlogo[1].png	
Category:	downloaded
Size (bytes):	697
Entropy (8bit):	7.573455613491714
Encrypted:	false
SSDEEP:	12:6v/7CZCVY4qjw64PjBxIpZDyGhCRGk0gOEsX09+tg+I/fux2KMiHxqDCDl3MAuk9:bZCVY4qjA7BGZDjhC0hVEKS+I+71RVCq
MD5:	E8F6445B7B7F0B26B63CD135E8BB3B3D
SHA1:	52C38CDD5696EE485D076F1B0FE40032B1BC608D
SHA-256:	089AA7FA65A4038B4AB9130D083E6BCC24B0E33F5018984EF1463B8516BC7993
SHA-512:	9AECE19461CF95558FA97EB0D7FB9D7CB5133FC31D651F76EA8B29986B4EBD1FB9D70B6D35DB13EFB9E27E0F6C71595D54B029E8673A37C39329450AF2898B76
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://plateflippers.com/OH2/GG8/images/microsoftlogo.png
Preview:	.PNG.....IHDR...s.....f.F...KPLTE...sss..3~.....=..>...O3....N3.O4.....{{{.....O3..$...)IDATH..... ....U.....KhE;....[Z.....@..#m..,g..l.->....-..._f..r.?..... 1... ....+.L.&1LD..&.g.q.....D.j..=.b.{...I....7...+.....{.....$.I.....4..m...B.Ef..v.....g3((c....r.....C'..]=.O.w...J$..3a..Dx.`.cY...1\..8k.IeZ.Z$...:..x..\.,.I.....-]^.g.1..8_Ke.D.....`b....a. KAr....y...p...U*3.+.%.`...za-.X8>.W..9g6..\0Q...7.....1R.(...bJ.:u..0.8.0.Po(.=N...)[s.1]..,.....V.ucN..P.K.4~.LY;..#..A.....Ll..*L.N..,D!_1C.U.Ju.....O.....C.JnO.^k/.).h.?....Pq.. '..2.)c..?&.9.\..k.s.I.....q6..}`.S.....U.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\office[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 512 x 512, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	6290
Entropy (8bit):	7.704429943211795
Encrypted:	false
SSDEEP:	192:5PesVaBqtC11xXiQU2SrR9PDD+2p4SWnR3m4UMWx:Zwyi3iQZSrRBDHmfHUMe
MD5:	1AC039422D7C9CEE436B2CAE5C00BD8C
SHA1:	60D9B9A6E2DF337578C35472344F1387775046D8
SHA-256:	1500514ADF9E666A3D20530815DF881BC94812C6906A53BD4C216D051D18C372
SHA-512:	03B225379AD1B46E3AF9AA3218812AED61D70431B17D75842E3CD426DBD960E940FB8C127F8D9DF7251039034A43848CE3EB612ED7B98D9A69050AF7CE7B0D7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://plateflippers.com/OH2/GG8/images/office.png
Preview:	.PNG.....IHDR.....$.....PLTE....'..)..'.,..)..*..*..(..(..)..-..'..(..(..)..*..)..*..-..*..'..)..+..+..+..,..,..+..(..,..+..+..+..+..+..(..+..+..*..,..<.....8..'..:.....zQ.....5..;..2..0.....8.....9..7. .6.....@..2..I..5..F..P..B..8.....M..e5.0...q.*.4..1.....c.X%.T .3..,.....j..X..y.].oC.a0.../..+.....~....-..wM.i;.:.....=.....sH....I?.5.....(.....7..2..;..:..*..0.....)tRNS..... .....cVPA-...\jfsH..7z=.s;....IDATx...i..A...gfr..ksm...e2..$fF...[RH.$. l9.UTa.../...E.;..}.....t.....*...=..L4#...i..&.m.....#...l%DA..]..... .=.zn.....h n.....q.v.....5....o..J!.,.....]..5....n....n.iw].....M..r$....n.i....k..Z&R... ..]Q.....+.....5P.hq.....J..;:...Zv..A..M.\.._s.Q2Z.=.....Z...).....,.....t.o..".&.,.....RK$.%m...Cm{ n.DQ...:0....$..)..7.v...@5\....n=.y.pU.....UIY.:x...*.H...{.X%.Uc..>.X.....>..K.x.....6.i.l.`.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\outlook[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 213 x 211, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1746
Entropy (8bit):	7.472505060810825
Encrypted:	false
SSDEEP:	48:lq3EkZ80zZgcSoWu+NIG208DXIbsXzVLp:qEGZgcMMGx8DYgXBp
MD5:	CACDEE9959D34380D727718FD02B3711
SHA1:	EB971467C555EA2299CC31018C8BC85F67DA59D7
SHA-256:	17F02FDB590800C9A21E2B6166F5F22CC54952D58897F09D8E82BB9195BC2071
SHA-512:	4F0A4BB3219BA1F9AAE6B527B9125FEE3327BDCA82142DFC23E6E6C5F4481065A221291A35BBCF1E35CFE9EE658AB22E4BC85DC58C17A2B95C5FC2846986FB66
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://plateflippers.com/OH2/GG8/images/outlook.png
Preview:	.PNG.....IHDR.....!.....PLTE.....T...2tRNS...Ji.Gd.=.@....X.g...\:. ..aMC.....}!.u'.P.5.S...p*Gi2....IDATx...is.@...n.....}.#.f...[t....qa...[.E.&O..A*.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.Y.U.....=.....aU..c...T..b.ztPu.;.ytPY.f..tP-....@U..... h..S....TVn .ytP9... ..s..h.....j\Z.D.....j...A...#..B"...HE..HE*!R.*$R.J.T...TiQ.!.,.....^%....4...2..ei...L.U..b.HG.k.N....V...4:W8.Q.1.V.Tmx./.I.../UeN.n*dN}.T...P...._..H...h.....T]._]..q>.O... Cu.....s W.jU....p.....".....BU..*..!..*S...P'.p...Q..~E.*i....E%.....U..>Q..j.B.q.%..q...T....j.Q.P..O....\..U.8j.JT...!2....KV.....*l.....{....JF-..<Y...Q.t.OSL.....U.%*.....OO,.-.H.....E.-i....g.Y."U3|9.'...A.J..Q.W./..G5z.H.]...:%MA...%.t...BC|f..e...3.0.]._f-.QPMPeG.4..;....[.(u*.{.F.W..L...r.Q=P..{.8G.Y0..X..gMP.._.3@...u.*...[....@.j.c.Y.P!L..w.#a.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\webmaillogo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 322 x 50, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	2869

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\webmaillogo[1].png	
Entropy (8bit):	7.911258790344632
Encrypted:	false
SSDEEP:	48:zUrFP7iiGbmCytjS8WTZgoQWY+BCJdfJCSrUyGfwZAq53AQkvQg9wTIIs9:zUrd7JG8tOLTyoQj+B5SrUfe1pg9wTIh
MD5:	85F7EBDACD174413927BD4B787997558
SHA1:	B03207C7F3EA92E9EA0EBDC2F804947CC726965D
SHA-256:	E298D32D99708F56D68EF9CD0C44EC85910A4DF7552B5B2041FCAA48D5EE9742
SHA-512:	0806DCF23E25EF775838F30C919ABB18E49B889E24EC56FA1045EFE26406C595A13E98B437A6E0BF87A3EE66888D6B37A14825500D93C856973F4BB3C5F7818E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://plateflippers.com/OH2/GG8/images/webmaillogo.png
Preview:	.PNG.....IHDR...B...2.....&".....PLTE.i3.....t7.P.l.....n3.m3.q3....|C...v:....Y.I.....y.b....e.....T.x>.....}.....s.q..].M.....i.....%.E...HIDATh..m{.@..gR...B" B.z."......#..ds...k...'..F...;>T...[..pX.s.....y.d?...s[..:\....P.1.h..~...)...T.5.....v.....(1.S.D....Lh[z`.W.mz.....%D.X"0..`..0)v..=..D....y..7..B.X..Z.`h.....\.t.....*.d.:.G...r....X&&..`...c. .....K..."d...W...V...]....7jk...Eh.p..\..s..).~.....T.....~+6..".uJx.<.x..k.q..pB.....*..u.%.6%.-.....?e9B#.odJ..Pl|Y.....:-...20..)#..$jm4...%l.fJ.I."{..W.{.....\&.....*.,.p.pj.K.[...n.o'\.Z...*4 .Oz....%..r).C..v...8...#2.....<.a.z.IT[h^M...E./6..G^.._.v.~0ju..b..j.....k9..\..3.8..S.9...-.H..):O..~Sw...;).jr.....K..F...~.m&u..iD...!0..j...o..>..i.2..P>mWG.{..!."..I...Rx..B[g. U.}s.g..s...o....G...)~...,....1..$.....<...b.`.....Qu...w5.X..].oQQ.%3*....~.=.%.1e....N..U..`@..m%....LR"K.#....:.8c*...D..._..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	144877
Entropy (8bit):	5.049937202697915
Encrypted:	false
SSDEEP:	1536:GcoqwrUPyDHU7c7TcDEBi82NcuSELL4d/+oENM6HN26Q:VoPgPard2oENM6HN26Q
MD5:	450FC463B8B1A349DF717056FBB3E078
SHA1:	895125A4522A3B10EE7ADA06EE6503587CBF95C5
SHA-256:	2C0F3DCFE93D7E380C290FE4AB838ED8CADFF1596D62697F5444BE460D1F876D
SHA-512:	93BF1ED5F6D8B34F53413A86EFD4A925D578C97ABC757EA871F3F46F340745E4126C48219D2E8040713605B64A9ECF7AD986AA8102F5EA5ECF9228801D962F5D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://plateflippers.com/OH2/GG8/css/bootstrap.min.css
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors. * Copyright 2011-2018 Twitter, Inc.. * Licensed under MIT (https://github .com/twbs/bootstrap/blob/master/LICENSE). */:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--orange:#fd7e14;--yellow:#ffc107;-- green:#28a745;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--primary:#007bff;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;-- warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoint-xl:1200px;--font-family-sans-serif:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol";--font-family-monospace:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monospace}*,::after,::before{box-sizing:border-box}h tml{font-family:sans

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\bootstrap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	46653
Entropy (8bit):	5.34222480854161
Encrypted:	false
SSDEEP:	768:JVCgM5KXrrcsU0n3fEHVAqcy6jOD0Ydkg+/ONU65Z+o+fSNx7eXs/ZWSMEMGLle9:JVjMyrcsU0nvRJOhzGqNxi8/866
MD5:	0827A0BDCD9A917990EEE461A77DD33E
SHA1:	6107D146E54A67C9998230ABF839301575D05702
SHA-256:	FA421B6EBBD2FB474D3A3866409CE6C1EFD120B47FF256FFFB8F8F50D556D3D9
SHA-512:	B3E3C2B2CFC0458AD8EC9957D4A78CF09C660163317F10BC786CFE014D2104A7AAE3D2DA2F898B6CCB20FFF0385604D9E47E1C410D492BFECAB667993BBA72 7A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0-alpha.6/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v4.0.0-alpha.6 (https://getbootstrap.com). * Copyright 2011-2017 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery. jQuery must be included before Bootstrap's JavaScript.");+function(t){var e=t.fn.jquery.split(" ")[0].split(".");if(e[0]<2&&e[1]<9||1==e[0]&&9==e[1]&&e[2]<1||e[0]>=4)throw new Error ("Bootstrap's JavaScript requires at least jQuery v1.9.1 but less than v4.0.0")}(jQuery),+function(){function t(t,e){if(!t)throw new ReferenceError("this hasn't been initialised - super() hasn't been called");return!e||"object"!=typeof e&&"function"!=typeof e?t:e}function e(t,e){if("function"!=typeof e&&null!==e)throw new TypeError("Super expression must either be null or a function, not "+typeof e);t.prototype=Object.create(e&&e.prototype,{constructor:{value:t,enumerable:!1,writable:!

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1887

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\css[1].css	
Entropy (8bit):	5.187998229445049
Encrypted:	false
SSDEEP:	48:SY3QW9Y3QLZY3QxTGY3QC7Y3Qw6QOWGOLpOxTvOChOw6b:SYgW9YgLZYgxTGYgC7Ygw6QOWGOLpOxo
MD5:	7AD11B51C8A9918ADE502DA9DE063EFF
SHA1:	ABF598711588628073EE60E294F288AB76EA187A
SHA-256:	5A270BD50EF12A93ABAE711C806D6C59D58B0E0D2A9B3463A8268DC3D2EA6857
SHA-512:	6932EACAB01B2443439A31537BC694BB6F611473BE6FC702DBCA92BC2DE27736F2A363744F14CCCDE7C05E660ACCADDA66523E5068371EFBDD8551B2375458A
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKWyV9hrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/opensans/v18/mem6YaGs126MiZpBA-UFUK0Zdcs.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 600;. src: url(https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKXGUdhrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKWiUNhrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 800;. src: url(https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKW-U9hrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\mem6YaGs126MiZpBA-UFUK0Zdcs[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17440, version 1.1
Category:	downloaded
Size (bytes):	17440
Entropy (8bit):	7.962704570077627
Encrypted:	false
SSDEEP:	384:2QHZz7pdg60gyjkXImq2+GTFGc+Hq8pMG2dKQWS:9HTyAYa+GIHzyKQX
MD5:	06B4BFDA4E139EAF3AB9872A6D66F42F
SHA1:	E5C5999D6AF4869BC60EEA92D1A8C328FB0E1378
SHA-256:	39EC493A5A688A85B60A1E889A22CFB93F23C900E0FDC0BE8AB8543DC9DAA783
SHA-512:	D6665B3CDD7E759D4A2B1BF916654A9C7FCA24ACBEBA1FB4A75668F5B451C7542B5683C097A6A62ACCE76B98694A4F6847CE2DC5193113D02200A04EC85A658
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem6YaGs126MiZpBA-UFUK0Zdcs.woff
Preview:	wOFF.....D .....d@.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....]...`~l.=cmap...`.....X..cvt .....W.....fpgm...l.....~a..gasp.....#glyf... ...4...M..o*.head..< ...6...6..z.hhea..<X..."...$. ..hmtx..<|...*.....=A.loca..>.....\|.maxp..@h... ... .name..@.....%`@.post..At.....x.l..prep..C0.....T..... .....x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`f.f.....:....Q.B3_dHcb```.fccfeabbi``P..x.....:;302(...&.O.....)B..q>H..u..R``..?i.....x.\.!..q..... .#aff...#1Q@.'U..@5.".llt.Aa#.f\|c.W....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..l;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$KY...e@.,.." ...?.....g....Z...[..5..=.d.....p.a.C?C..L...FF~..,...x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...s.3.S...co..o.~.Zy.u...kW.\.t...N.KG.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\memnYaGs126MiZpBA-UFUKWyV9hrIqU[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17668, version 1.1
Category:	downloaded
Size (bytes):	17668
Entropy (8bit):	7.9576211916710635
Encrypted:	false
SSDEEP:	384:TQHZiJiLqdJVOpEbXHYV0cIeLg8hDHNbCqe+WQN:NWuV1X/eRHNbCqefQN
MD5:	793B1237017AEACD646FB80911425566
SHA1:	51E3023140BE407FD5FBFD27E0A5D2C30AE66F31
SHA-256:	5BB07410994C14D60F72CE3F6E19B172FCD7BC515F9BAEAF1F74C6CC2216E86A
SHA-512:	95C6644C1C1A2E369075D429E86736491451431C6046BA74545C0BF91C1CABEA1B1A4FCFD8FC5BB6A37269E4F80AF5B792BF80C968EC6A3B8B325F33EC66331
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKWyV9hrIqU.woff
Preview:	wOFF.....E.....c.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....]...`~...cmap...`.....X..cvt .....^.....M..fpgm...t.....~a..gasp.....#glyf... ..4...Lv$.#.head..<....6...6./{.hhea..=...."...$....hmtx..=4...@....}.K.loca..?t.....*maxp..A4... ... .name..AT.....*.D9post..BD.....x.l..prep..D.....$...J..... .....x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.%..@@.@.....T.2..Q.1dB...!.j@..}(../y..]...V....b.b.D#5/....(..v.p...'e.7.....@@?.9.....x.\.!..q..... #aff...#1Q@.'U..@5.".llt.Aa#.f\|c.W....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..l;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c.. .P...,..`....b`....C ..D@$P..)._.....a .p@.0.(.@.8. ..0....a8.....x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...s.3.S...co..o.~.Zy.u...kW.\.t...N

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\memnYaGs126MiZpBA-UFUKXGUdhrIqU[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17492, version 1.1
Category:	downloaded
Size (bytes):	17492
Entropy (8bit):	7.957749340429713

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\memnYaGs126MiZpBA-UFUKXGUdhrIqU[1].woff	
Encrypted:	false
SSDEEP:	384:bQHZhYs3a6PsVt9W9Z3owyC3bSZjyVO9Gz8W6EaJQgacXcK1cDVQgx:gq6PMK9Z3WCyc5z6lnXcYcxQU
MD5:	56E5756B696615D6164A625E1BCB1A9E
SHA1:	E2AEF56F577DBB78254066B73C2D0FBE30B40AE0
SHA-256:	BB87838929C15E1D0A05693C375323B95B6B4690FE207D3639E3A432C44AEF35
SHA-512:	BB998858AB9DF11375B0844EA008D31ABE4377826F6BE73C6F1DDE2E85C6F9A0404FADFDA9C081318F2F59614A22A1CF7F32376B25232887EDE8C7FBA323CB1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKXGUdhrIqU.woff
Preview:	wOFF......DT......dD........................GDEF................GPOS...............GSUB.......X...t...OS/2.......]...`.7.rcmap...`.........X..cvt ....^........fpgm...t........~a..gasp................glyf......4 ..M4.]2.head..<<...6...6..zghhea..<t..."...$.{.@hmtx..<....,.....V9Vloca..>.........rimaxp..@.... ... .name..@.........,G.post..A........x.I..prep..CT........x..%.................................... ..x...5.A......m."gW..`.L..&N".?.......IF....a.^...b1.................Uh."4...>..=x.c`f........:....Q.B3_dHcb```.fgc.`abbi``P..x......:.;302(...&.O.....)B..q>H.%.u..R``..<......x.\.!..q......#aff...# 1Q@.'U..@5.".llt.Aa#.f\|c.W.....'..X..!..C...ITPE.;..V.j......0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e(}.IS2..uc]p.........M.x.c.a.g.c..$KY...e@.,A.".m....x........3 ....[.o....=.d...u.a......S....G..3.b..h...."...x.uTGw.F........)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...s.3.S...co..o.~.Zy.u...kW.\.t...N

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\officebg[1].jpg	
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, 1420x1080, frames 3
Category:	downloaded
Size (bytes):	199781
Entropy (8bit):	7.986685505356506
Encrypted:	false
SSDEEP:	3072:GqroO3SvvO1a2DzHMuaXi8NHYpw97qefRS1XATbNr31uR+lGjcobBKTyl6XUV1:Uvv69Mlxpd5qXAThr31urDboT/q1
MD5:	058E25C4AA0FCCB6A280E543B4C108E8
SHA1:	05AF10D488E0651737E4AE510DF17DA2166463DA
SHA-256:	7A2C0B0E1E16041B12DD1A7D18438CEB14063C980799BAEE1D55CB2F04892777
SHA-512:	D98759E65DA318FD8092B5E03C9875FB782C7DBA4C01DD85FCACFA4E5747F2C105A96F04C9032F977554229D425CBBA9254692CB5AA4841F401BCC31A481FE7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://plateflippers.com/OH2/GG8/images/officebg.jpg
Preview:	......JFIF.............C..........................%!'&$!$#).;2),8,#$3F48=?BCB(1HMH@M;AB?...C...........?*$*??......8...." ....X.>.....:...p..:....Q...Q.......b.[...Q.@.9.8t...).T..a......+....t...YC...;0+H.D...V......7Q........].P.............:........;.............t9..FH.T. 93...qj-....*.."r..Wst.Pj.6.Q..J.....j0.c.....?@(S...........9.X.>jQ...}(...J_....../Dc.E.@.@9.8t+.Bxt..(...w...0.1@....(. a..(......[..>..=..;....u..v>~._.."...+..t.Wc<L&.(J . ...V..L. ....:......s..0......`j..!'..?P...:..qX.....tf.L.5&...f.....&_T.O.jnf.K.S3..-I.7s.:fp.dQ:.e..9........(....8..............t.{.w..%F.F.A.FR..T......@.......B..s................z>~.N............1....7P...0.8.HF... ..>........N.w.t........:0....Kf......$..@O...j.....4`H..D.K...rk'.F..."'*Pi.8._....N.......{Q.3...dEp.K]....H.k...f.V$n.s.t8..!q..@..?...|.....>..q...y>....@...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\officelogo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 163 x 75, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1223
Entropy (8bit):	7.435397013783005
Encrypted:	false
SSDEEP:	24:gidVU+bg/fKMNezOpBlETR/CjB3EUlKd1i4hDHm+IH7AsbX:gidVU+M/CisOTlzjB3EUlK/iqmrH7R
MD5:	8DB2ADD18C0D34794B35DEEE1FDC14DB
SHA1:	6E72801F98A832E9193A4D9F4389AEAE1E5233DD
SHA-256:	EFACCC2B190FCCE0F0AB41064D882FB4A701C6AED6B1035595A16138E32A0A50
SHA-512:	FC0FEC864045DE68E355E61E3DDAFB103BA5E2ABCD5838ECCB80AEB55200F4659719A15CF25E1BCEC1F631B0F4F4319F18C662E526714E9EBBF56131CC7AEA 05
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://plateflippers.com/OH2/GG8/images/officelogo.png
Preview:	.PNG........IHDR.......K.....+..]....PLTE....<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..<..< ....1tRNS..a....Y.+..}...p2...T...gJ!..v^.=9...D&.O..8.......IDATh...0.FCep@.AP..q.z.....B..V.-....?.....D...@ ....D3.&.3.5..).C...E...t...{..l}..r...?....c../.I/..e...\........{..#..5n.....r.r ....1........W.v....b}Lf.e."5.(H..a...K.?..rc........rG...m.>......X.%J.......gA..."?.........}...W...u....y..U..1cW..!........W.f...3....`...4....+..px(..Q.T.N......M...6.qeU..y.t........4X.5...........+... cs..8..-.U&h.n.._..w..i`..!....(a.}E.N(_o`L.78.l76..c......Zq.."2...b...n.'...".tkN..op..:..Gv..2.*.2.w..8...Z..A+.O..{G.E.....<.5w......G.1..j..`...k2.;juG....W.A..H...T...........3.i=v.g.! `5C..+.....1.Y(.g..X?.S4.v...C..EF<s\.Q.1..9Y.;...8...'.......}mUY......4{.........8%O.W@N8;z..9..g...o...#96.e...".3..vG..)Ug.]...G.O+Z...w.x../;&..8r.P...~.).8...b.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	10084
Entropy (8bit):	5.0668781976760915
Encrypted:	false
SSDEEP:	192:4Sz3ZfziAkFTF5bkJq0QU9esLFcqH72V2LFs:4a3ZPkFTF2g0X9ZLFjRs

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\style[1].css	
MD5:	9D8F3FCC24C20CA06678AD500BF55150
SHA1:	E0100DE345BCFA97AF7C15957D7BC1B2BBE91061
SHA-256:	CC4703F492AA58E929D57812FD5A8580258006E0121DD097E866B4EE38A800AA
SHA-512:	39E2611748104EFBF9F90EC4242DF3BA33176C80B2A61343F69746F34D0FAF4E2967E5D3129F4430963AE1D2CBE3CDCC1BD6D6ECEA2D00436B1FD76364138A5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://plateflippers.com/OH2/GG8/css/style.css
Preview:	@import url('https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400i,600,600i,700,700i,800,800i');...wrap {..overflow:hidden;.}.a:hover,a:focus {..text-decoration:none;.}..btn:focus {..box-shadow: none;.}.img {..max-width:100%;.}..webmaillogo.{. text-align: center;.}..webmaillogo img.{. margin-top: 125px;.}..webmailloginform.{. width: 300px;. margin:20px auto;.}..orangeclr .input-group-addon.{. color: #ec6933;. border-color: #ec6933;.}..orangeclr .form-control.{. color: #ec6933;. border-color: #ec6933;.}..orangeclr .form-control:focus.{. border-color: #ec6933;.}..mainpage.{..background: url("../images/landing-devices-bg.jpg");..background-repeat: no-repeat;..background-size: cover;.}..onedriveform.{..background: #1082df;..padding: 20px 70px 50px 70px;..min-height: 100vh;.}..logo.{..text-align: center;.}..logo img.{..margin-top: 31px;.}..onedriveform p.{. font-family: 'Open Sans', sans-serif;. text-align: center;. color: #fff;. font-siz

C:\Users\user\AppData\Local\Temp\~DF2B39EDCB32CC438A.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF8ADC395168C1F92B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	63865
Entropy (8bit):	0.9188112259436093
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+11JZILvlD/eB/8T/eB/8ilLGs3z8+j1emqJK1emjaK1em0m+OwT3O:kBqoxKAuqR+11JZILvBbaFRIJGBXNcb
MD5:	5582856D044B69E3ADAC4EB9BAFEC6AC
SHA1:	8588EB79B3B33B414A2F3ACC6B9BC6879E245A0C
SHA-256:	5BCB627A23821A0C1415239E896C4327FA46AFEB3AD3C3DB22EA831B0F6A9C77
SHA-512:	2CB2E846C129E3D0B483B9BF0114927F0149D47C6D7DBC3D18754F4CA835712B79153E2F201C65B87A88F9D7FDD96E55094F2AA54B3018843A4891754D86EE67
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFE69385337526499A.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4792445119342846
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loE39loE39lWErhIih+L+JCgm:kBqoIE4EmErhIih+L+kgm
MD5:	365522B40BE6DAAB01E930C30A2644B2
SHA1:	BE37B4155E1F1D550D1645876D4A124D6054CEED
SHA-256:	F86B78A69AAB23F374EB14C60AEAA7E3AD2941AC88F1ABBD37EC67E5E6932B48
SHA-512:	6922F2D0F0388AB40F9FCC1D2D332223172D397B05F4342E6A19CFFA2FA17A03500D6DAF989511E0A79C89DB94D4D167B3F4711ED79E44B8B909EA3024DB4B3
Malicious:	false

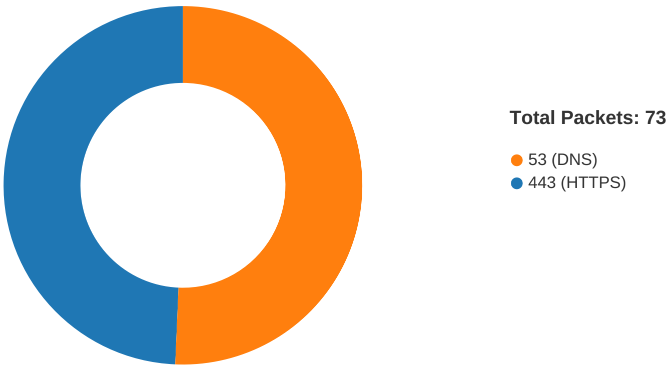
C:\Users\user\AppData\Local\Temp\~DFE69385337526499A.TMP	
Reputation:	low
Preview:	...............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 15:40:21.925283909 CET	49745	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:21.925287962 CET	49746	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.080992937 CET	443	49746	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.081027031 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.081168890 CET	49746	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.082835913 CET	49745	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.088716030 CET	49746	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.088794947 CET	49745	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.244204044 CET	443	49746	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.244277000 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.244519949 CET	443	49746	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.244539976 CET	443	49746	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.244559050 CET	443	49746	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.244573116 CET	443	49746	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.244609118 CET	49746	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.244667053 CET	49746	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.245510101 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.245541096 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.245558977 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.245572090 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.245608091 CET	49745	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.245706081 CET	49745	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.245943069 CET	443	49746	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.246087074 CET	49746	443	192.168.2.4	162.241.127.18

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 15:40:22.247111082 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.247200966 CET	49745	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.316813946 CET	49746	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.317047119 CET	49745	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.326936007 CET	49745	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.472378016 CET	443	49746	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.472482920 CET	49746	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.472959042 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.473061085 CET	49745	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.507105112 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.507139921 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.507157087 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.507174015 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.507188082 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.507200956 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.507209063 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.507230043 CET	49745	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.507276058 CET	49745	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.751672029 CET	49745	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.755789995 CET	49746	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.757770061 CET	49748	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.907931089 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.907964945 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.907982111 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.907999992 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.908016920 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.908039093 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.908057928 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.908058882 CET	49745	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.908073902 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.908092022 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.908109903 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.908126116 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.908128023 CET	49745	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.908144951 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.908159018 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.908168077 CET	49745	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.908178091 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.908200979 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.908216953 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.908217907 CET	49745	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.908235073 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.908252001 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.908252954 CET	49745	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.908310890 CET	49745	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.911618948 CET	443	49746	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.911658049 CET	443	49746	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.911674976 CET	443	49746	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.911690950 CET	443	49746	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.911709070 CET	443	49746	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.911725044 CET	443	49746	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.911730051 CET	49746	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.911741972 CET	443	49746	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.911763906 CET	443	49746	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.911793947 CET	49746	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.911838055 CET	49746	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.913677931 CET	443	49748	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:22.913798094 CET	49748	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.955301046 CET	49746	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:22.956063032 CET	49748	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:23.064028978 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:23.064053059 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:23.064065933 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:23.064080954 CET	443	49745	162.241.127.18	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 15:40:23.064099073 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:23.064114094 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:23.064131021 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:23.064147949 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:23.064163923 CET	49745	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:23.064167976 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:23.064203024 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:23.064219952 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:23.064235926 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:23.064243078 CET	49745	443	192.168.2.4	162.241.127.18
Mar 5, 2021 15:40:23.064254999 CET	443	49745	162.241.127.18	192.168.2.4
Mar 5, 2021 15:40:23.064274073 CET	443	49745	162.241.127.18	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 15:40:12.930804968 CET	62389	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:12.988049030 CET	53	62389	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:13.926597118 CET	49910	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:13.975606918 CET	53	49910	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:14.796444893 CET	55854	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:14.845297098 CET	53	55854	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:15.902805090 CET	64549	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:15.948796988 CET	53	64549	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:16.971963882 CET	63153	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:17.022155046 CET	53	63153	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:18.329969883 CET	52991	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:18.375907898 CET	53	52991	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:19.278851032 CET	53700	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:19.327676058 CET	53	53700	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:20.527775049 CET	51726	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:20.585863113 CET	53	51726	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:20.834220886 CET	56794	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:20.881577015 CET	53	56794	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:21.856381893 CET	56534	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:21.912323952 CET	53	56534	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:22.267868042 CET	56627	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:22.315452099 CET	53	56627	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:22.836850882 CET	56621	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:22.883930922 CET	53	56621	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:23.261934042 CET	63116	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:23.326730013 CET	53	63116	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:23.775393009 CET	64078	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:23.792659044 CET	64801	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:23.825432062 CET	53	64078	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:23.851978064 CET	53	64801	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:24.734538078 CET	61721	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:24.783262968 CET	53	61721	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:25.697102070 CET	51255	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:25.746011019 CET	53	51255	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:26.850549936 CET	61522	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:26.898125887 CET	53	61522	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:28.397434950 CET	52337	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:28.445770025 CET	53	52337	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:29.969969034 CET	55046	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:30.033843994 CET	53	55046	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:31.311924934 CET	49612	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:31.357763052 CET	53	49612	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:33.111208916 CET	49285	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:33.156971931 CET	53	49285	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:40.281363010 CET	50601	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:40.287848949 CET	60875	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:40.333647013 CET	53	60875	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:40.353718042 CET	53	50601	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 15:40:41.413455963 CET	56448	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:41.460839033 CET	53	56448	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:42.535918951 CET	59172	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:42.581626892 CET	53	59172	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:43.731962919 CET	62420	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:43.780461073 CET	53	62420	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:43.941543102 CET	60579	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:43.989077091 CET	53	60579	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:50.515904903 CET	50183	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:50.561851025 CET	53	50183	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:51.359803915 CET	61531	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:51.408869982 CET	53	61531	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:51.534477949 CET	50183	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:51.580421925 CET	53	50183	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:52.367631912 CET	61531	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:52.417249918 CET	53	61531	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:52.552819014 CET	50183	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:52.607367992 CET	53	50183	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:53.383151054 CET	61531	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:53.432879925 CET	53	61531	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:54.539599895 CET	50183	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:54.585587978 CET	53	50183	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:55.399234056 CET	61531	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:55.449534893 CET	53	61531	8.8.8.8	192.168.2.4
Mar 5, 2021 15:40:58.556458950 CET	50183	53	192.168.2.4	8.8.8.8
Mar 5, 2021 15:40:58.603877068 CET	53	50183	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 5, 2021 15:40:21.856381893 CET	192.168.2.4	8.8.8.8	0xa98	Standard query (0)	plateflippers.com	A (IP address)	IN (0x0001)
Mar 5, 2021 15:40:22.836850882 CET	192.168.2.4	8.8.8.8	0xe50	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Mar 5, 2021 15:40:23.775393009 CET	192.168.2.4	8.8.8.8	0x2016	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Mar 5, 2021 15:40:40.281363010 CET	192.168.2.4	8.8.8.8	0x3fc4	Standard query (0)	plateflippers.com	A (IP address)	IN (0x0001)
Mar 5, 2021 15:40:43.731962919 CET	192.168.2.4	8.8.8.8	0xb4fa	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 5, 2021 15:40:21.912323952 CET	8.8.8.8	192.168.2.4	0xa98	No error (0)	plateflippers.com		162.241.127.18	A (IP address)	IN (0x0001)
Mar 5, 2021 15:40:22.883930922 CET	8.8.8.8	192.168.2.4	0xe50	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 15:40:23.825432062 CET	8.8.8.8	192.168.2.4	0x2016	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Mar 5, 2021 15:40:23.825432062 CET	8.8.8.8	192.168.2.4	0x2016	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Mar 5, 2021 15:40:40.353718042 CET	8.8.8.8	192.168.2.4	0x3fc4	No error (0)	plateflippers.com		162.241.127.18	A (IP address)	IN (0x0001)
Mar 5, 2021 15:40:43.780461073 CET	8.8.8.8	192.168.2.4	0xb4fa	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Mar 5, 2021 15:40:43.780461073 CET	8.8.8.8	192.168.2.4	0xb4fa	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	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
Mar 5, 2021 15:40:22.245943069 CET	162.241.127.18	443	192.168.2.4	49746	CN=plateflippers.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Mar 04 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Thu Jun 03 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Mar 5, 2021 15:40:22.247111082 CET	162.241.127.18	443	192.168.2.4	49745	CN=plateflippers.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Mar 04 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Thu Jun 03 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Mar 5, 2021 15:40:24.068531036 CET	104.16.19.94	443	192.168.2.4	49760	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
					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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 15:40:24.087296009 CET	104.16.19.94	443	192.168.2.4	49758	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	Thu Oct 21 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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		
Mar 5, 2021 15:40:40.677321911 CET	162.241.127.18	443	192.168.2.4	49770	CN=plateflippers.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Mar 04 01:00:00 CET 2021	Thu Jun 03 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Mar 5, 2021 15:40:43.883320093 CET	104.18.10.207	443	192.168.2.4	49777	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	Tue Mar 01 00:59:59 CET 2022	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		
Mar 5, 2021 15:40:43.885514021 CET	104.18.10.207	443	192.168.2.4	49778	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	Tue Mar 01 00:59:59 CET 2022	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 15:40:43.886296988 CET	104.18.10.207	443	192.168.2.4	49779	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		

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: iexplore.exe PID: 6904 Parent PID: 800

General

Start time:	15:40:18
Start date:	05/03/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff778860000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6960 Parent PID: 6904

General

Start time:	15:40:19
Start date:	05/03/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6904 CREDAT:17410 /prefetch:2
Imagebase:	0x1140000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly