ID: 432783
Cookbook: browseurl.jbs
Time: 18:42:41
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

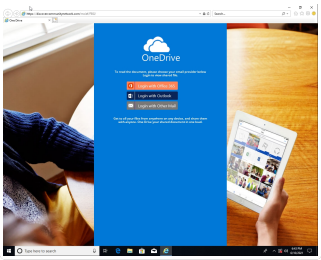
Analysis Report https://discovercommunitynetwork.com…

Overview

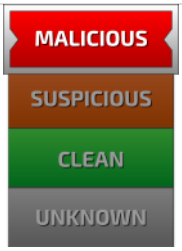
General Information

Sample URL:	http://https://discovercommunitynetwork.com/mcief/FBG
Analysis ID:	432783
Infos:	

Most interesting Screenshot:



Detection



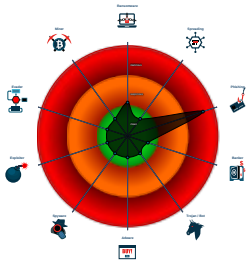
HTMLPhisher

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Phishing site detected (based on sh…
- Yara detected HtmlPhish7
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- Invalid T&C link found

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 4644 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1724 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4644 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\9QTQHWWN\FBG[1].htm	JoeSecurity_HtmlPhish_7	Yara detected HtmlPhish_7	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
- Antivirus detection for dropped file

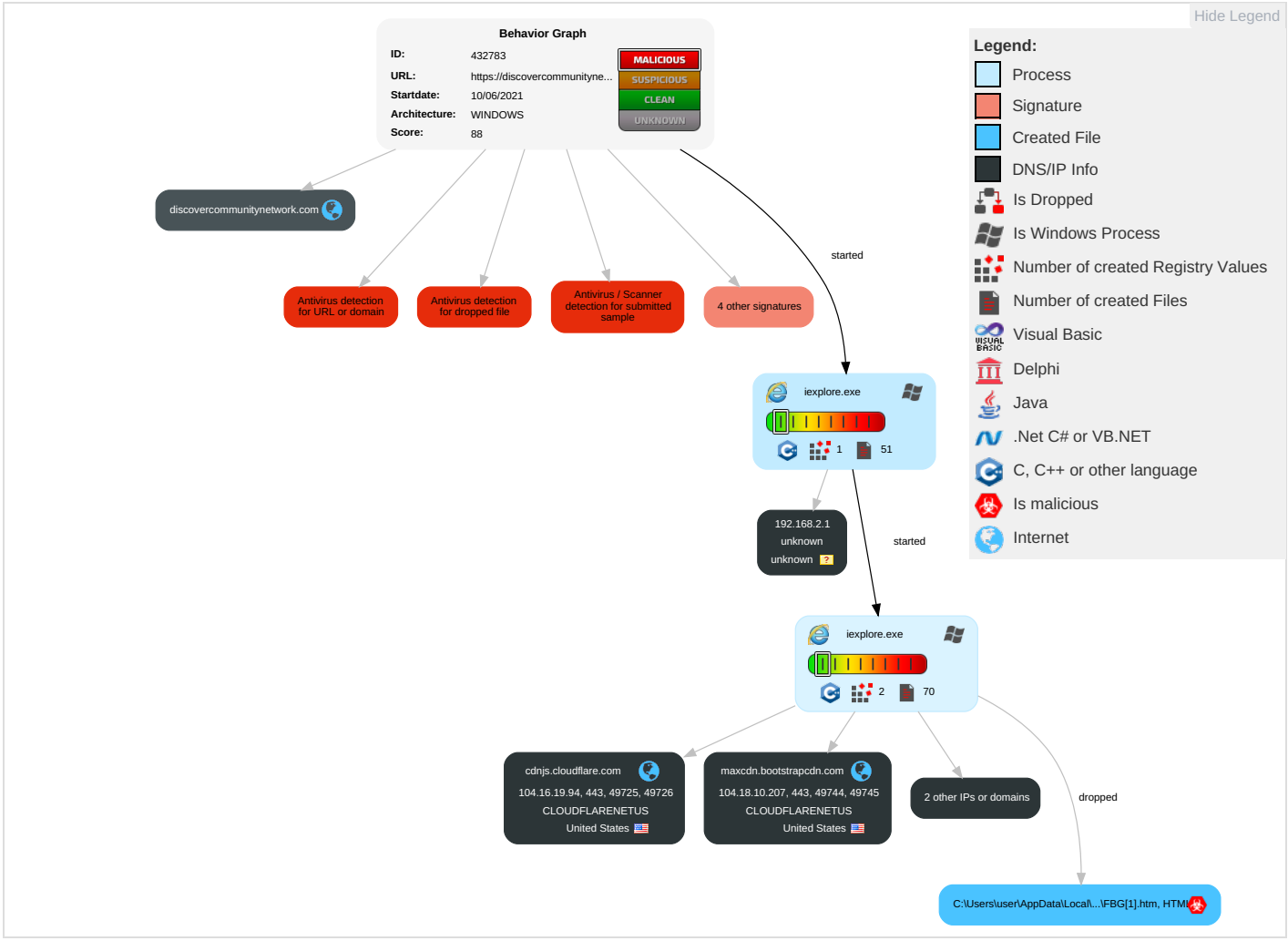
Phishing:

- Phishing site detected (based on shot template match)
- Yara detected HtmlPhish7
- Phishing site detected (based on image similarity)
- Phishing site detected (based on logo template match)

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

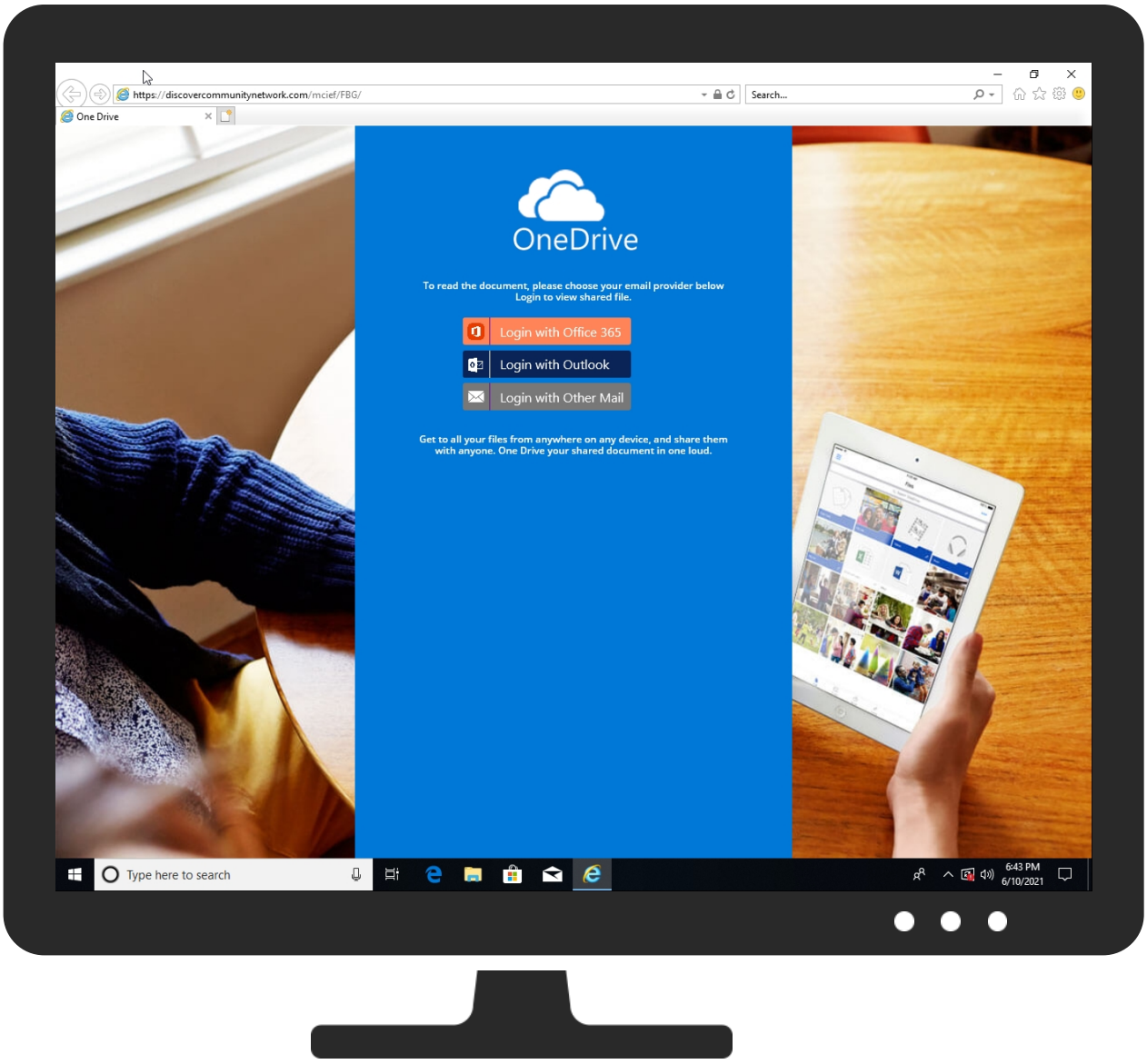
Behavior Graph



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://discovercommunitynetwork.com/mcief/FBG	0%	Virustotal		Browse
http://https://discovercommunitynetwork.com/mcief/FBG	0%	Avira URL Cloud	safe	
http://https://discovercommunitynetwork.com/mcief/FBG	100%	SlashNext	Fake Login Page type: Phishing & Social usering	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\FBG[1].htm	100%	Avira	HTML/Infected.WebPage.Gen2	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
discovercommunitynetwork.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://discovercommunitynetwork.com/mcief/FBG/microsoft.php	100%	SlashNext	Fake Login Page type: Phishing & Social usering	
http://https://discovercommunitynetwork.com/mcief/FBG/	100%	SlashNext	Fake Login Page type: Phishing & Social usering	
http://https://discovercommunitynetwork.com/mcief/FBG/webmail.php	100%	SlashNext	Fake Login Page type: Phishing & Social usering	
http://https://discovercommunitynetwork.com/mcief/FBG/office.php	100%	SlashNext	Fake Login Page type: Phishing & Social usering	
http://https://discovercommunitynetwork.com/mcief/FBG/webmail.phpv	0%	Avira URL Cloud	safe	
http://https://discovercommunitynetwork.com/mcief/FBG/office.phpwork.com/mcief/FBG/office.php	0%	Avira URL Cloud	safe	
http://https://discovercommunitynetwork.com/mcief/FBG/k.com/mcief/FBG/	0%	Avira URL Cloud	safe	
http://fontawesome.iohttp://fontawesome.iohttp://fontawesome.io/license/http://fontawesome.io/licens	0%	Avira URL Cloud	safe	
http://https://discovercommunitynetwork.com/mcief/FBG/webmail.php://discovercommunitynetwork.com/mcief/FBG/	0%	Avira URL Cloud	safe	
http://https://discovercommunitynetwork.com/mcief/FBG/microsoft.phpBSign	0%	Avira URL Cloud	safe	
http://https://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://discovercommunitynetwork.com/mcief/FBG/itynetwork.com/mcief/FBG/microsok.com/mcief/FBG/	0%	Avira URL Cloud	safe	
http://https://discovercommunitynetwork.com/mcief/FBG/itynetwork.com/mcief/FBG/webmailk.com/mcief/FBG/	0%	Avira URL Cloud	safe	
http://https://discovercommunitynetwork.com/mcief/FBG/itynetwork.com/mcief/FBG/office.k.com/mcief/FBG/	0%	Avira URL Cloud	safe	
http://https://discovercommunitynetwork.com/mcief/FBG/Root	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdnjs.cloudflare.com	104.16.19.94	true	false		high
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
discovercommunitynetwork.com	77.79.239.202	true	false	• 0%, Virustotal, Browse	unknown
code.jquery.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://discovercommunitynetwork.com/mcief/FBG/microsoft.php	true	• SlashNext: Fake Login Page type: Phishing & Social usering	unknown
http://https://discovercommunitynetwork.com/mcief/FBG/office.php	true	• SlashNext: Fake Login Page type: Phishing & Social usering	unknown
http://https://discovercommunitynetwork.com/mcief/FBG/webmail.php	true	• SlashNext: Fake Login Page type: Phishing & Social usering	unknown
http://https://discovercommunitynetwork.com/mcief/FBG/	true	• SlashNext: Fake Login Page type: Phishing & Social usering	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.10.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
77.79.239.202	discovercommunitynetwork.com	Poland		15694	ATMAN-ISP-ASATMSAPL	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432783
Start date:	10.06.2021
Start time:	18:42:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://discovercommunitynetwork.com/mcief/FBG
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:	7
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:	mal88.phis.win@3/42@5/4
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://discoverc ommunitynetwork.com/mcief/FBG/office.php • Browsing link: https://discoverc ommunitynetwork.com/mcief/FBG/microsoft.php • Browsing link: https://discoverc ommunitynetwork.com/mcief/FBG/webmail.php
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{6D04534A-CA56-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.849220558899609
Encrypted:	false
SSDEEP:	96:rqZZpZz2pW1Gt1AqAf16Hz1MforTf4xRfNI+ffzH+lX:rCZpZz2pWUtqfUhMymTfbcX
MD5:	3E952076D7125601E1E0382E935E49F3
SHA1:	AFBCBA4597FD7D23A976194A17F483457A49B7F1
SHA-256:	0184D0D697B73E672C7C4E1924C72C81A37108D00FEB0E250D8DD028D9CF223D
SHA-512:	0D4CF387E5442BEF254B84E21260185C7BA0BAA59B5CAD7575F0C2CEE13963AD4BD5CF8914F718E0EBF0CD13AB8315BA3AB1A4210FC196B8058D2058B82B2E9C
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\{6D04534C-CA56-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	67860
Entropy (8bit):	2.249127087386567
Encrypted:	false
SSDEEP:	384:r4o+OPwcClkj7FS2r3aa5krcEqQQDbP16ZeTVXN0:G
MD5:	AC1095BD35CBAAB0015CB1B12B2B08E7
SHA1:	A423E4042E6C2DD400AA7842E905C1FE4D0801F4
SHA-256:	406976993B450BEC12021FC39F141C46882924D7E26AE7D7B2D1865C3C4A446D
SHA-512:	AD230235FF9711E5D203B33079E5D19D7186E12C7128D9F3B8EB8E872D1B7B06982A19956E6CF446512E16FF071E523190075DC7722F330855B9126AEF5B7BDF
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\{6D04534D-CA56-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5648367912316608
Encrypted:	false
SSDEEP:	48:IwLjGcprWGwpajjG4pQrGrapbSlGQpKnG7HpRnTGIpG:rLZZOQjV6fBSPAGTVA
MD5:	343A0BCCF2D62CDE047DF2C79F18DC7F

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{6D04534D-CA56-11EB-90E5-ECF4BB2D2496}.dat	
SHA1:	6A7A97E6875B44DF313D028B3C9E33946E57F54C
SHA-256:	7CDCC924349D7AF09EBEB1E0DE0156D521E179A6B22CF2A576EE64C69B666D37
SHA-512:	FB43EC66C2CDABF96BCE0F0B74DB5190ED72BA5EE049D4835DBFC8E7433CF43CEC5D3E00A5E99A1E3CF46BF0EC7BB7A6C7516C1275276EBE9DD276328C0B750F
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\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://discovercommunitynetwork.com/mcief/FBG/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\3Y2ADQKS\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://discovercommunitynetwork.com/mcief/FBG/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}html{font-family:sans

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\jquery-3.1.1.slim.min[1].js	
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\3Y2ADQKS\mem5YaGs126MiZpBA-UN8rsOUuhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19160, version 1.1
Category:	downloaded
Size (bytes):	19160
Entropy (8bit):	7.967047296085223
Encrypted:	false
SSDEEP:	384:wQDywW7WywLbHesuDAL7df4V7G/aSpBpucg7KInWtKgqp/y:6wW7LkrescWgG/DuJmIWtKgi/y
MD5:	ADC0530936D8C9AA4279699007BBBEDB
SHA1:	A25B788600D5F280B0B79A93BC1116A667BAC7D6
SHA-256:	012A20DD3CC6D96015C9D5896EEA6DA97D841E940ABA5F13BC0C43AB6F9D0FB0
SHA-512:	0B768871575BAC86528E1DAA477D0E231907627116C292F4C017990AC49B9D847F866324BD95F3DF8B75F02FB97474336A5BDB844D8867956113702B434D2EFD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v20/mem5YaGs126MiZpBA-UN8rsOUuhv.woff
Preview:	wOFF.....J.....qD.....GDEF.....GPOS.....GSUB.....y....;..OS/2...$...^...`...vcmap.....Y..cvt ...8...g.....o.[fpgm.....s.ugasp...D.....#glyf...T..:F..Y.%..Ohead..B....6...6....hhea..B.....$....hmtx..B....-....(..C.loca..E$.....maxp..F.... ... .name..G.....%.@cpost..H.....5.".prep..I.....1..S.....x.M...P.@..L..$$. .g..;..k.z...P.$K.....[.E..Z....B)..a.:...i...!.....J ...U....l/..m.&*3.KO...#..-..%;7.V.....x.c`f.cV``e``..j...(.../2.11s01qs.1s.01.400.300x.....:.;380(...&.O...)B..q>H.%.u..R``.....x.\.!..q.....#acf...#1Q@.'U..@..".llt.Aa#.f|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$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]..|..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\memnYaGs126MiZpBA-UFUKWiUNhrIqU[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17512, version 1.1
Category:	downloaded
Size (bytes):	17512
Entropy (8bit):	7.968196019099005
Encrypted:	false
SSDEEP:	384:TLq60uOF2lS+F0tIAj23Km+GwptAko/13pSJn2IpCEApitRVE9ZtIKZ:bS2c+ZAj26m+Gw/ot5SJn2l83iEZ
MD5:	AE9D2F1CE08FBDF103EE860763B106FF
SHA1:	2E16DAE015C60EFA97ACF4CCC628F798C4981AB9
SHA-256:	7263F989C49E7C621C73468B7DDDEB14497B529EDF427DE520EF636A2224FAC9
SHA-512:	6FBE7566AB26401EA987F4CA761275D15BF931B049A92EABBF832F72065D8C40CF151878CEBA5C030BB06EE0609F5CB0CF6BDBB979657DA8E4B747ADCC9FED63
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v20/memnYaGs126MiZpBA-UFUKWiUNhrIqU.woff
Preview:	wOFF.....Dh.....e.....GDEF.....GPOS.....GSUB.....y....;..OS/2...$...]..`....cmap.....Y..cvt ...8...b.....g.ifpgm.....s.ugasp...@.....glyf...L..3...NX.r..head..<L...6...6..{.hhea..<....."...$...bhmtx..<....-...../.loca..>.....8maxp..@.... ... .y..name..@...../)/C.post..A.....5.".prep..Cx.....x.M...P.@..L..$$. .g..;..k.z...P.$K.....[.E..Z....B)..a.:...i...!.....J ...U....l/..m.&*3.KO...#..-..%;7.V.....x.c`f9.....u..1...<.f.....b.. 0t.vfPdP...M...C.G/S....|..K..6 .....t...\.\.!..q.....#acf...#1Q@.'U..@..".llt.Aa#.f|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$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..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\memnYaGs126MiZpBA-UFUKXGUdhrIqU[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17556, version 1.1
Category:	downloaded
Size (bytes):	17556
Entropy (8bit):	7.960906849962957
Encrypted:	false
SSDEEP:	384:8rQHZcYO3tzgQrjWqkQBoYSzsKXd/URVA2WqqqImx:zMpgQ+qBoYSzrXdODr
MD5:	95042C5DB55DB8390646FCBA3898BCB4
SHA1:	EB31C4EACA9BD696299D85CA329F0DBAE887FF8F
SHA-256:	F5180DA3A46CF194294D3FCDF522A418ED78458D332332A6D9D827ADA1589D3F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\memnYaGs126MiZpBA-UFUKXGUdhrIqU[1].woff

SHA-512:	D3CC14DFF1D4832C045011E2A4850101898682FF1884C4C2155AC57D6A4550C243020735F3C52EE5406F47D9C2113D3C3460BFB3A31A0AF5AF8A0EC5E90E04E8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v20/memnYaGs126MiZpBA-UFUKXGUdhrIqU.woff
Preview:	wOFF......D.......d........................GDEF................GPOS...............GSUB.......y.....;..OS/2...$..]...`.7.rcmap............Y..cvt ...8...^........fpgm............~a..gasp...4............glyf.. .@..4*..MD.&..head..<l...6...6..zghhea..<...."...$.{.Ahmtx..<..../......9.loca..>...........maxp..@.... ... .name..@.........G.post..A.........5.".prep..C.........x..%......................... ....x.M...P.@..L..$$. .g..;..k.z...P.$K......[.E..Z....B)..a.:...i...!......J ...U....l/..m.&*3.KO...#..-..%;7.V..........x.c`f........:....Q.B3_dHcb```.fgc.`abbi``P..x......:.;302(...&.O... ..)B..q>H.%.u..R``..<......x.\.!..q......#acf...#1Q@.'U..@..".llt.Aa#.f\|c.W.....'..X..!..C...ITPE.;..V.j......0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$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...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\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
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:	9AECE19461CF95558FA97EB0D7FB9D7CB5133FC31D651F76EA8B29986B4EBD1FB9D70B6D35DB13EFB9E27E0F6C71595D54B029E8673A37C39329450AF2898B7 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://discovercommunitynetwork.com/mcief/FBG/images/microsoftlogo.png
Preview:	.PNG........IHDR...s..........f.F...KPLTE...sss..3~........=..>...O3....N3.O4............{{{...................O3..$...)IDATH..... ....U........KhE;....[Z.....@..#m..,.g..I.->....-..._f..r.?..... 1... ....+.L.&1LD..&.g.q...............D.j..=.b.{...I....7...+.....{......$.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\3Y2ADQKS\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:	FC0FEC864045DE68E355E61E3DDAFB103BA5E2ABCD5838ECCB80AEB55200F4659719A15CF25E1BCEC1F631B0F4F4319F18C662E526714E9EBBF56131CC7AE 05
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://discovercommunitynetwork.com/mcief/FBG/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\3Y2ADQKS\style[1].css

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	10088
Entropy (8bit):	5.06703500664872
Encrypted:	false
SSDEEP:	192:4Sz3RzYAkFTF5bkJq0QU9esLFcqH72V2LFs:4a3nkFTF2g0X9ZLFjRs
MD5:	E4C124F84BE2A66C6069E569257E6CF3
SHA1:	E9B6E3207CEAF681F763A49EBCD71837A8EA5CFB
SHA-256:	4DA858A3EC305F55BAFB14B408E69398AE8E7AA76AC67025EEC6A2534C592B64
SHA-512:	7C5C533AECBC3865B4794411256D2AAC628E7AB9AA508C3E06FCCED49F2F6B46D1D7719944F914C63D9332C9F40493A6DDAE5B1BAD2532E4D547960EDF67FD D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\style[1].css	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://discovercommunitynetwork.com/mcief/FBG/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;.}..we bmailloginform.{. 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;.}..onedrivepage.{..background: url("../images/landing-devices-bg.jpg");..b ackground-repeat: no-repeat;..background-size: cover;.}..onedriveform.{..background: #0078d7;..padding: 20px 70px 50px 70px;..min-height: 100vh;.}..logo.{..text-align: ce nter;.}..logo img.{..margin-top: 31px;.}..onedriveform p.{. font-family: 'Open Sans', sans-serif;. text-align: center;. color: #fff;. font

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\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
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://discovercommunitynetwork.com/mcief/FBG/images/webmaillogo.png
Preview:	.PNG.....IHDR...B...2.....&".....PLTE.i3.....t7.P.l.....n3.m3.q3....|C...v:....Y.l.....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..)#..$jm4...%l.fJ.l."{..W.{.....\&.....*.,.p.pj.K.[...n.o'\.Z...*4 .Oz....%..r).C..v...8...#2.....<.a.z.IT[h^M...E./6..G^.._.v.~0ju..b..j.....k9..\..3.8..S.9...-.H..):O..~Sw....;).jr.....K..F...~.m&u..iD...!0..j...o..>..i.2..P>mWG.{..!.''..I...Rx..B[g. U.}s.g..s...o....G...)~...,....1..$.....<...b.`.....Qu...w5.X..].oQQ.%3*....~.=.%.1e....N..U..`@..m%....LR"K.#....:.8c*...D..._..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\FBG[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	2166
Entropy (8bit):	4.783348469787835
Encrypted:	false
SSDEEP:	48:4JvzHBDB6EVxh9UBuyptGQIVeeLYOOGnj:63T9UECErVLYk
MD5:	8E16ACA17D79C4A7BBC9A76A49119560
SHA1:	DC4D66B46EDCAC7E747F5923D8838C91818C33E7
SHA-256:	84F1D1FFDC036768FFEBA1BE92362DCF619E7CE6EC27500AB47844ED24FC4230
SHA-512:	8E177DE65CF480E390C93CB4FB623F581612B8B596C04C7513E728C5493F8249A47D8ADA89A0E1CEB034291C80A7FB1960DE718FF896A33019A223E09CF65482
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_7, Description: Yara detected HtmlPhish_7, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\FBG[1].htm, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
IE Cache URL:	http://https://discovercommunitynetwork.com/mcief/FBG/
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>.. Bootstrap CSS -->. <link rel="stylesheet" href="cs s/bootstrap.min.css">. <link rel="stylesheet" type="text/css" href="css/style.css">. jQuery first, then Tether, then Bootstrap JS. -->..</head>.<body>..<div cl ass="onedrivepage">. . . . . <p>To read the document, please

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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+iiHML6YVA30UtEMH2Utl:JGP7iA+jML6YVA30UtEMH2Utl
MD5:	7E923AD223E9F33E54D22E50CF2BCCE5
SHA1:	8B7CB193D70BB476DB06651C878DFCD1A7E1C0EE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\bootstrap.min[1].css	
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\9QTQHWWN\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\9QTQHWWN\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1887
Entropy (8bit):	5.180102741405681
Encrypted:	false
SSDEEP:	48:SY3QWeY3QLGY3QxTVY3QCMY3Qw6XOWjOLQOxTSOCMOw6u:SYgWeYgLGYgxTVYgCMYgw6XOWjOLQOx9
MD5:	F0DFBF035F5547DFF41229F461471228
SHA1:	BA54747E3E95B9D4957686D78DD266223AC7CAE5
SHA-256:	9DB4DCD3E0E45AD82801C1F61098610D7D6A1C56C6D8020F5C1CF62EDDDCB1A1
SHA-512:	AC3CBD20D428C1BA4DC0E2BB36E87E7EC73E6742D1B52D96010DF8A7EA86828F6E4FDED30FCCD433E8637078EBA48D015DA1DABCFA59637DFC399FECBF2E C6A6
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/v20/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/v20/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/v20/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/v20/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/v20/memnYaGs126MiZpBA-UFUKW-U9hrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\mem5YaGs126MiZpBA-UN7rgOUuhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19008, version 1.1
Category:	downloaded
Size (bytes):	19008
Entropy (8bit):	7.966749425699339
Encrypted:	false
SSDEEP:	384:IF/o+9PD3ixaac1lphLEanpKkfulibGLVEwUVV2LHxti+6epB:5MPD3iA9vpMk4ikOV2LzDrz
MD5:	396C9555F9EADB66270C25FC3157743F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\mem5YaGs126MiZpBA-UN7rgOUuhv[1].woff

SHA1:	D834DA7E230D9798071F8FABD0DB49ECD0A24BCC
SHA-256:	463DA44840BB99F312F92DBA6F39D259DD2669C9A2E45EB8086037B60EF31DED
SHA-512:	A490C3E5E735A1CAAFCD6C3E1DC321BCA6CC29E3F32EA414041F4B67166CA3D7DDC5D4C3A370A66A7447D943B72EBB59103875B9538314259680B1654085ADB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v20/mem5YaGs126MiZpBA-UN7rgOUuhv.woff
Preview:	wOFF.....J@.....qd.....GDEF.....GPOS.....GSUB.....y.....;..OS/2...$...^...`....cmap.....Y..cvt ...8...].....-..fpgm.....s.ugasp...<.....glyf...H..:...Z@ ..>head..BL...6...6.%l.hhea..B.....$.)..hmtx..B.....OYloca..D.....maxp..F.... ... .r..name..F.....#.>.post..G.....5.".prep..IX.....k.....x.M...P.@..L..$$. .g..;..k.z...P.$K.....[.E..Z....B)..a.:...i...!.....J ...U....l/..m.&*3.KO...#..-..%;7.V.....x.c`f.g.....:....Q.B3_dHc.....@`...../..?....^..... 9.8.m@J....w..!..x.\.!..q.....#acf...#1Q@.'U..@..".llt.Aa#.f|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..l;o..<.$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.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\mem5YaGs126MiZpBA-UNirkOUuhv[1].woff

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18784, version 1.1
Category:	downloaded
Size (bytes):	18784
Entropy (8bit):	7.964699694030365
Encrypted:	false
SSDEEP:	384:4YQHZJ+ZXshfYjP0lJ9WnX/zJuKvvaIYjSS4yKrtVIGPvRGq6:BchgjGJ9WnX/zJ1JcG3gf
MD5:	CA0CC58FE4C481D2486F836E8B7ACD98
SHA1:	B9988071248F824BA2D5FA88CB16DA1971AA0945
SHA-256:	B332B402229655660F0DDC7D916618F44ACA71D0ECAA68A1DF7B5AD5A5F1D6F9
SHA-512:	95E3C7674FFF4E934F252605CD3DCDF169986EE754964C703F1BFEAD52AB33F8DFE3764A8FD507E39E4C058985CCC90F6B0F69A766AAA1C8508DB806095904A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v20/mem5YaGs126MiZpBA-UNirkOUuhv.woff
Preview:	wOFF.....I`.....nl.....GDEF.....GPOS.....GSUB.....y.....;..OS/2...$...^...`.-..cmap.....Y..cvt ...8...[.....4fpgm.....~a..gasp...0.....glyf...<..9...WXZ..uhead..AL...6...6...Mhhea..A.....$...$hmtx..A....#.....T.loca..C.....6.Kkmaxp..E.... ... .u..name..E.....#.@Ppost..F.....5.".prep..H`.....x..n.....x.M...P.@..L..$$. .g..;..k.z...P.$K.....[.E..Z....B )..a.:...i...!.....J ...U....l/..m.&*3.KO...#..-..%;7.V.....x.c`fy.....:....Q.B3_dHc.....@`...../..?....^..... 9..m@J.....x.\.!..q.....#acf...#1Q@.'U..@..".llt.Aa#.f|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..l;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$KY...e@.,A.".m....x.....3.....?.[.o...2...:...a..b.)@.Y.....v1.b4d...36 ..x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...s.3.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\mem6YaGs126MiZpBA-UFUK0Zdcs[1].woff

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17504, version 1.1
Category:	downloaded
Size (bytes):	17504
Entropy (8bit):	7.960726283242655
Encrypted:	false
SSDEEP:	384:gOQHZDOjNtkrTZx8YbwLPGK+miKq4EpS5syMVdSNI8S:/tkrTBbSq4ZsyY
MD5:	531BF97B28201ADDC0C05AF57A953F15
SHA1:	53C3B719C96FE1913A38CF1EBCFA3EA93699853F
SHA-256:	887661900A506AF06D17741BC2649A4AA578C9268BB2730C9E05F0155456CFF2
SHA-512:	3842158808C21BC798A89DA009459AD4C17DA319493B0FA467A1FA66308C306BEBA89A43E4B714BE781A16F68EEFFE1EFD0EA0AAE06BD53F26F03D4A49F10905
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v20/mem6YaGs126MiZpBA-UFUK0Zdcs.woff
Preview:	wOFF.....D`.....d.....GDEF.....GPOS.....GSUB.....y.....;..OS/2...$...]...`~l.=cmap.....Y..cvt ...8...W.....fpgm.....~a..gasp...,.....#glyf...<..4...M....head..<T...6...6..z.hhea..<....".$. . hmtx..<.....=B.loca..>.....?. maxp..@.... ... .name..@.....%`@.post..A.....5.".prep..Cp.....T.....x.M...P.@..L..$$. .g..;..k.z...P.$K.....[.E..Z....B )..a.:...i...!.....J ...U....l/..m.&*3.KO...#..-..%;7.V.....x.c`f.f.....:....Q.B3_dHcb```.fccfeabbi``P..x.....:.;302(...&.O....).B..q>H..u..R``..?i.....x.\.!..q.....#acf...#1Q@.'U..@..".llt.Aa#.f|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..l;o..<.$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...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\memnYaGs126MiZpBA-UFUKWyV9hrIqU[1].woff

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17732, version 1.1
Category:	downloaded
Size (bytes):	17732
Entropy (8bit):	7.957222623966965
Encrypted:	false
SSDEEP:	384:+vDQHZiYwiPYuU+kEvu/A3WTzOhDGnUdBZmQMuEM+PIH:+VULU+keWWsqhDGQmFw
MD5:	7774AE48788CA5B876E5D2BD35367401

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\memnYaGs126MiZpBA-UFUKWyV9hrIqU[1].woff	
SHA1:	EC805AADB15B1A74BBCA28180C4347A6623C10C2
SHA-256:	91B6F4F34465AEEBDA712B48CB01CF3ABB5AC0090B4DD9464E68790A69F55570
SHA-512:	1EB7CC117E497F01A749522B83092EEC563CB7F73F153777582111D2E48C86E439BCDB6D341D4A35D7A3F88D7E336FD2731932CDDA55C557247A0F4B9186C71
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v20/memnYaGs126MiZpBA-UFUKWyV9hrIqU.woff
Preview:	wOFF.....ED.....c.....GDEF.....GPOS.....GSUB.....y....;..OS/2...$...]...`~...cmap.....Y..cvt ...8...^.....M..fpgm.....~a..gasp...4.....#glyf.. .D..4...L..I.1head..=....6...6./{.hhea..=@...''...$....hmtx..=d...C....;LEloca..?.....maxp..Al... ... .name..A.....*.D9post..B|.....5.".prep..D@.....$...J..... .....x.M...P.@..L..$$. .g..;..k.z...P.$K.....[.E..Z....B)..a.:...i...!.....J ...U....I/..m.&*3.KO...#..-..%;7.V.....x.%..@@.@.....T.2..Q.1dB...!.j@..}(../y..]...V....b.b.D#5/...(..v.p ....'e.7.....@@?.9.....x.\.!..q.....#acf...#1Q@.'U..@..''.llt.Aa#.f\|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.... .....M.x.c.a.g.c.. .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...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\webmail[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:	C1D80614AEAE0E47083897421190828B3E9043F6
SHA-256:	C7A2BC42652E4C60BFD5F2E4D3A3D8111F1602B3C0C4E04E010D6E32B869645D
SHA-512:	8265B855FF0C4987F19728040CC29F1C01ADAA1EAE4C1B50D255F274BD6CDDE4BCC6C6C27FE16A4B4FFF3E7CD2DC44AA1832B798739178F420302651ABF113 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://discovercommunitynetwork.com/mcief/FBG/webmail.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="ht tps://code.jquery.com/jquery-3.1.1.slim.min.js" integrity="sha384-A7FZj7v+d/sdmMqp/nOQwliLvUsJfDHW+k9Omg/a/EheAdgtzNs3hpfag6Ed950n" crossorigin="anony mous"></script>. <s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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://discovercommunitynetwork.com/mcief/FBG/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\G62TDH9B\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\fontawesome-webfont[1].eot	
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\G62TDH9B\landing-devices-bg[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, 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://discovercommunitynetwork.com/mcief/FBG/images/landing-devices-bg.jpg
Preview:	.....JFIF.....C.....!*$..(..%2%(,-/0/.#484.7*./....C..... ....=... @..... ....'.W].8 @..... .....hS....A J.....s.....2j.I.!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\G62TDH9B\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://discovercommunitynetwork.com/mcief/FBG/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\G62TDH9B\microsoft[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	9075
Entropy (8bit):	5.166298455927209
Encrypted:	false
SSDEEP:	96:RL9O4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDmxhGzoxLrPPDlcOyeBLYYnNdt72tR:x9ToSBjlevudl9nUwMxzNYYN/mma
MD5:	A2194596BA144676F157DE78DEE56319
SHA1:	444B66D24B6973D885637AEA0E4BD3FAEE726440

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\microsoft[1].htm	
SHA-256:	24D9D15532B55CBA48F65813F4376E718C1B39B33D525F085B1A138C8D424181
SHA-512:	52941BA78FB57FFCE081E80E88DF15B37F1F8824981D88714D2636167303E3C8E7C1945C5217BCAD0D9FF6EDE97DCE8C017D808218189EEEFACF345348E72D4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://discovercommunitynetwork.com/mcief/FBG/microsoft.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>. .. . .<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\office[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://discovercommunitynetwork.com/mcief/FBG/office.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\G62TDH9B\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://discovercommunitynetwork.com/mcief/FBG/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.$. l9.UTa.../...E.;..}.....t.....*...=..L4#...i..&.m.....#...l%DA..]....=.zn.....hn.....q.v.....5....o..J!.,....]..5....n....n.iw].....M..r$....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\G62TDH9B\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\outlook[1].png	
SHA-256:	17F02FDB590800C9A21E2B6166F5F22CC54952D58897F09D8E82BB9195BC2071
SHA-512:	4F0A4BB3219BA1F9AAE6B527B9125FEE3327BDCA82142DFC23E6E6C5F4481065A221291A35BBCF1E35CFE9EE658AB22E4BC85DC58C17A2B95C5FC2846986FB66
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://discovercommunitynetwork.com/mcief/FBG/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.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\OTUW0Q90\FBG[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	707
Entropy (8bit):	5.162345868595955
Encrypted:	false
SSDEEP:	12:hYYLszHjgfkbxsjJ7QCdToh50lXQoLYlJl5M6eNsJLi334VlKk:hYYIzDIkejNQCRtgoLY95MI5634Vsk
MD5:	1304294C0823CA486542BA408ED761E3
SHA1:	B2A70FB2D810CA13985882E6981F33998823E83E
SHA-256:	3BBE72F3BAA8EC61DE17A1D767FCA58704769684B7ABE9161D0C4EAF4C8F0982
SHA-512:	67430E967118D2B2D8A448C583BDE082BF512DA88EAE75B0501EC5A6C2B0BF46936306317BD3DDD956C5C6E01FE0C7DBED43927588EFBA06C5F84D8A557F7BB
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html style="height:100%">.<head>.<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />.<title> 301 Moved Permanently..</title></head>.<body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;">. . 301 . Moved Permanently.. . The document has been permanently moved. . </body></html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\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\OTUW0Q90\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:	dropped
Size (bytes):	207927
Entropy (8bit):	5.3700159283175415
Encrypted:	false
SSDEEP:	6144:qHxLZjYHvDU8CumHxLZjYHvDU8CumHxLZjYHvDU8Cur:CGMGMGZ
MD5:	1563DDAD57A8F6A2517A662965281204
SHA1:	B0935DADD1EE4C3446DFA43771A92821C5B255F3
SHA-256:	E8A6A5B1816BDD87692BAAA7CBA05957793FAD9BB9C854545A3C32F59CB4D7EB

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\jquery-3.1.1.slim.min[1].js	
SHA-512:	2B00B0A0DF4D758FA76387025BC83B2C587BA1442A09C4B00A623B1E85C4E90C1696BD5C1AD02412C74C1409E330C52E2B12653D4A59C96459767EA437AF16C
Malicious:	false
Reputation:	low
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\OTUW0Q90\mem5YaGs126MiZpBA-UN_r8OUuhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18744, version 1.1
Category:	downloaded
Size (bytes):	18744
Entropy (8bit):	7.966883926264397
Encrypted:	false
SSDEEP:	384:zawWpQHZNpxHreHjc5bHhYc9ON58zWZnmiN4RHcSd2UrrMKCWX:zawPscLqqO/8zG/4RHvdh33X
MD5:	2A6051095E2330FB1A45B836E3BA038E
SHA1:	1DA733C279AA12C3D8857AED80CD910C2B209EAE
SHA-256:	C98B647124C63DEA93B52BCF6A97A76A6944B9894DC0377B70F8C3B47D91382A
SHA-512:	CB019D3D69A51FE9522AA22BF637886B9691270F0BA409167B5A1225CB50BCE494ADEAACC7C94D341A02B3AC751620E9E6A4B9AD9B3FF916C3FA12D710A3AC6D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v20/mem5YaGs126MiZpBA-UN_r8OUuhv.woff
Preview:	wOFF.....l8.....n.....GDEF.....GPOS.....GSUB.....y.....;..OS/2...$...^...`}...cmap.....Y..cvt ...8...]....fpgm.....~a..gasp...4.....#glyf.. .D..8...W.._..head..A....6...6..F.hhea..AT.....$...dhmtx..At....._.loca..C.....K.`@maxp..EP... ... .name..Ep.....c?Jpost..F\.....5.".prep..H .....:.] .....x.M...P.@..L..$$. .g..;..k.z...P.$K.....[.E..Z....B).a.:...i...!.....J ...U....l/..m.&*3.KO...#..-..%;7.V.....x.c`fig.a`e``..j...(.../2.1..`b.ffcfeabbi``Pg``..b.. 0t.vfp`P...M... C.G/S....\|...=.6 .....m/....x.\.!..q.....#acf...#1Q@.'U..@..".llt.Aa#.f\|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$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...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\mem8YaGs126MiZpBA-UFVZ0d[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18160, version 1.1
Category:	downloaded
Size (bytes):	18160
Entropy (8bit):	7.961831708897042
Encrypted:	false
SSDEEP:	384:K9BQHZEFEbXlSNPoWvbYZbX9rnztP94u6pZ4nmrOmbSi+x:KLSb1GIbN76j4oO8j+x
MD5:	20890DE1FB4E49EA0B36F058BCA1B7E7
SHA1:	023D6720D92A54A3BB0AB219818D2E6E6AAD24A7
SHA-256:	C71180612EA84F5F9882D35DF024707E5B5E1BB18EFB2C8123FA5BDD30D3E079
SHA-512:	E6B921D20C0B7BFEA5A79D18D1C23DA7C79BB4E4D76A29AF48D7705C9C1F43E9E6578F1F36E00624DACD97411B68A214E750D0EDEB7BF12E889F16B6C522E1B0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v20/mem8YaGs126MiZpBA-UFVZ0d.woff
Preview:	wOFF.....F.....j8.....GDEF.....GPOS.....GSUB.....y.....;..OS/2...$...^...`~]..cmap.....Y..cvt ...8...Y.....M..fpgm.....~a..gasp...0.....#glyf.. .@..6...S.Ug:}head..>....6...6..cphhea..?$.....$....hmtx..?D.....[Xloca..Ad.....l.maxp..C,... ... .name..CL.....&:A.post..D<.....5.".prep..F.....C..... .....x.M...P.@..L..$$. .g..;..k.z...P.$K.....[.E..Z....B).a.:...i...!.....J ...U....l/..m.&*3.KO...#..-..%;7.V.....x.c`f..8.....u..1...<.f.....A.....5....1...A.._6..".-..L.....Ar ,.....3..(....x.\.!..q.....#acf...#1Q@.'U..@..".llt.Aa#.f\|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$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.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\memnYaGs126MiZpBA-UFUKW-U9hrIqU[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22088, version 1.1
Category:	downloaded
Size (bytes):	22088
Entropy (8bit):	7.976197045721412
Encrypted:	false
SSDEEP:	384:PnGPIpMdUGB5dC/q5f2Rh1T9+LraA27GnT4l5UcexDokQcH9slkDk1vRO2B:PnG5dzA/qN2RBIeA27GT4zAxDofcHeeY
MD5:	6B8620DD9B7F0DE6531FCC1D397B5361
SHA1:	15632276D3969AA6FCCC2231906FB44FA5479EB0
SHA-256:	FC849DBB5A6BC86E49018BF353EAACA1DDA58427F5A0ED6E6B6CFBD6F90ADB77
SHA-512:	F4F6656EA257477CB1584D788BA8E0B79CD439DC41FADE2C3FD234E3FE8C927D7C802E9D49F0CFA7E9992A50F1F2887560C937B117E617770F840D369087A378

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\memnYaGs126MiZpBA-UFUKW-U9hrIqU[1].woff	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v20/memnYaGs126MiZpBA-UFUKW-U9hrIqU.woff
Preview:	wOFF......VH...............................GDEF.......\........GPOS...........R.c..GSUB...d...s.....,.OS/2.......U...`t..%STAT...0...B...V^.B.cmap...t...........`cvt ...,.......8I.G.fpgm............. ..Zglyf......;...Z.....head..K....6...6...)hhea..KD...#...$....hmtx..Kh.......P..2,loca..N........*!..Nmaxp..P$... ... .name..PD...$...`;.^.post..Qh.......y0>r.prep..T....B......3)x.....@ ...}w.A...@.6.(t...A1T..i.. R@..Y...u.[1.ng/.%..J.]..M.=..K.K\|\|5....&:..1.f4..D..Mx.5....`...{zz.m.m.m.m.m...f.Nf....u!.B"+.._.h...G...c.V..I...A.......i....(.1...l......(.EH$F...Q.1....LY0. ....0..1..P.;p..../.....]....]C.8.R.KT.-.%.^...Yrje.-......R].Jci).e.t..[..{..ce.i.^...TV.^.m.(.m{XN.y.j....>.O...Z#R.5.&.Tz... U\...k.f.....Z;jw....F.x......\.*...G..^..zW..K....+....X.lJF$]r)9..".0. ..)L..\L.g....I.........{&-...<........$......Ny/.)W...~...g.C.YL...D.!....../Y.\...R...7.9(.....@......x...../w.zpu#..,72.L...z7.......=g....M.& .Y...F..n.cCN.`'.K..o.......}A>.{

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\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://discovercommunitynetwork.com/mcief/FBG/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\OTUW0Q90\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://discovercommunitynetwork.com/mcief/FBG/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..-l.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\OTUW0Q90\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
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:	1EC6758BDBE5A34D656DA7BE28897FFFA28FC6438EEB148F2363DE7EC6620BC2E6496F4A0D63182BD8E136A13D5EC6E31B2AE740067AB121EFB67475DAC24F 8C
Malicious:	false
Reputation:	low

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\tether.min[1].js</th></tr>
<tr><td>IE Cache URL:</td><td>http://https://cdnjs.cloudflare.com/ajax/libs/tether/1.4.0/js/tether.min.js</td></tr>
<tr><td>Preview:</td><td>!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 s
trict";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=ge
tComputedStyle(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</td></tr>
</table>

C:\Users\user\AppData\Local\Temp\~DF6E29A9E8804300A7.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	64941
Entropy (8bit):	0.8887466826765789
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+IOEV+xji14xFaa53fa5MSF8SbQW+2:
MD5:	719EF09F1CDB0B40024B131F7EA3E4E1
SHA1:	7820AA3576DC678EF9356A32DD7DF35B8D6DC9ED
SHA-256:	67D80DB0C524EEB3A635E7E61164FB7DD03AC2DFF45186BC061FBC8CF28BEF0F
SHA-512:	E65C2155EA87695B47D4704DF6B1875A656011B7BC70FDBF9CEB6003A70AC311B2C42336E1165FD441CE4EF0F7A9F7A67138C3BAA2D532371DD9E4C67BC1E1 A
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF7D600D7A9EE5F323.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\~DF8F906952B71A6755.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4769399542625979
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loC9loy9lWGGD2vG97z69goi:kBqoItrGw2vO7zKTi
MD5:	0EAD1EF684F9C5939E3AEEB4C7C90A75
SHA1:	506CEE847B35CFA9B4ED39DD578257C02A91D2F8
SHA-256:	B5D2DCCF3C620562345D7C46ED634B920A7A5A9E218A8F097DA57B27BDC7D0C1
SHA-512:	130ED46A762C0C8C591B6A241DF52C7B7249CB75D3D78C0EC92CF896F8CFE7D7CE338403115D780720D7BBCE61CFC242CFCD32BF46A957ED5406A3ED0A56F 5C
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 18:43:34.533204079 CEST	192.168.2.6	8.8.8.8	0x2b12	Standard query (0)	discoverco mmunitynet work.com	A (IP address)	IN (0x0001)
Jun 10, 2021 18:43:35.423283100 CEST	192.168.2.6	8.8.8.8	0xf28f	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jun 10, 2021 18:43:35.472043991 CEST	192.168.2.6	8.8.8.8	0x2bf6	Standard query (0)	cdnjs.clou dflare.com	A (IP address)	IN (0x0001)
Jun 10, 2021 18:43:51.496695042 CEST	192.168.2.6	8.8.8.8	0x7f89	Standard query (0)	discoverco mmunitynet work.com	A (IP address)	IN (0x0001)
Jun 10, 2021 18:43:54.237535954 CEST	192.168.2.6	8.8.8.8	0x23d4	Standard query (0)	maxcdn.boo tstrapcdn.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 18:43:34.610130072 CEST	8.8.8.8	192.168.2.6	0x2b12	No error (0)	discoverco mmunitynet work.com		77.79.239.202	A (IP address)	IN (0x0001)
Jun 10, 2021 18:43:35.476499081 CEST	8.8.8.8	192.168.2.6	0xf28f	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 18:43:35.532077074 CEST	8.8.8.8	192.168.2.6	0x2bf6	No error (0)	cdnjs.clou dflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jun 10, 2021 18:43:35.532077074 CEST	8.8.8.8	192.168.2.6	0x2bf6	No error (0)	cdnjs.clou dflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jun 10, 2021 18:43:51.555165052 CEST	8.8.8.8	192.168.2.6	0x7f89	No error (0)	discoverco mmunitynet work.com		77.79.239.202	A (IP address)	IN (0x0001)
Jun 10, 2021 18:43:54.298595905 CEST	8.8.8.8	192.168.2.6	0x23d4	No error (0)	maxcdn.boo tstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Jun 10, 2021 18:43:54.298595905 CEST	8.8.8.8	192.168.2.6	0x23d4	No error (0)	maxcdn.boo tstrapcdn.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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 10, 2021 18:43:34.751456022 CEST	77.79.239.202	443	192.168.2.6	49720	CN=discovercommunitynetwork.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	Sun Apr 11 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Jul 11 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		
Jun 10, 2021 18:43:34.751502037 CEST	77.79.239.202	443	192.168.2.6	49721	CN=discovercommunitynetwork.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	Sun Apr 11 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Jul 11 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		
Jun 10, 2021 18:43:35.675751925 CEST	104.16.19.94	443	192.168.2.6	49726	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
Jun 10, 2021 18:43:35.749775887 CEST	104.16.19.94	443	192.168.2.6	49725	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		
Jun 10, 2021 18:43:51.677232981 CEST	77.79.239.202	443	192.168.2.6	49743	CN=discovercommunitynetwork.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	Sun Apr 11 02:00:00 CEST 2021	Sun Jul 11 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		
Jun 10, 2021 18:43:54.390166998 CEST	104.18.10.207	443	192.168.2.6	49746	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		
Jun 10, 2021 18:43:54.390204906 CEST	104.18.10.207	443	192.168.2.6	49744	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
Jun 10, 2021 18:43:54.391474009 CEST	104.18.10.207	443	192.168.2.6	49745	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

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 4644 Parent PID: 792

General

Start time:	18:43:31
Start date:	10/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 1724 Parent PID: 4644

General

Start time:	18:43:32
Start date:	10/06/2021

Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4644 CREDAT:17410 /prefetch:2
Imagebase:	0xc90000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Disassembly