ID: 322950
Cookbook: browseurl.jbs
Time: 06:18:23
Date: 26/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

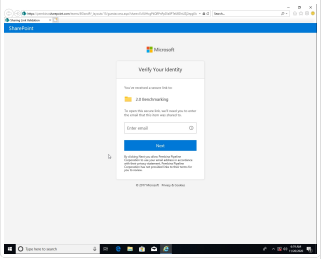
Analysis Report https://pembina.sharepoint.com/teams/...

Overview

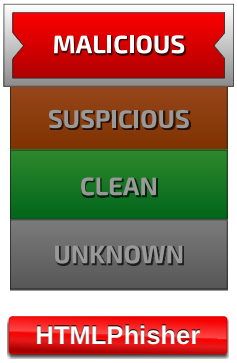
General Information

Sample URL:	https://pembina.sharepoint.com/teams/BOandP/_layouts/15/guestaccess.aspx?sh...s.aspx?share=Ev8UHcgPkQRPnPpDIa8PTeUBDnUZj2epg0IcLzD6O0XQNQ&e=5:GyiSQ3&at=9
Analysis ID:	322950

Most interesting Screenshot:



Detection

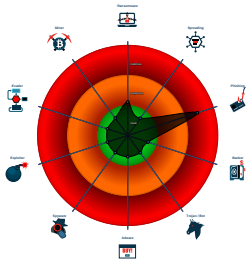


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish_10
- Phishing site detected (based on im...
- Phishing site detected (based on log...
- HTML body contains low number of ...
- HTML title does not match URL
- Submit button contains javascript call

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6772 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6816 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6772 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 7144 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6772 CREDAT:82952 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- dllhost.exe (PID: 6260 cmdline: C:\Windows\system32\DllHost.exe /Processid:{49F171DD-B51A-40D3-9A6C-52D674CC729D} MD5: 2528137C6745C4EADD87817A1909677E)
  - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

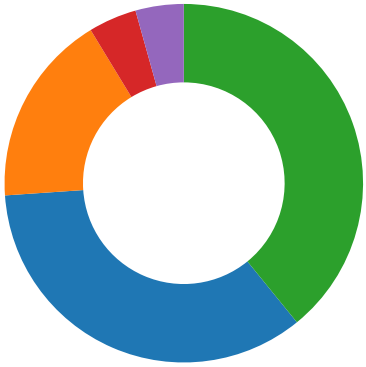
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\guestaccess[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- Phishing
- Networking
- System Summary
- Malware Analysis System Evasion
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

Phishing:

Yara detected HtmlPhish_10

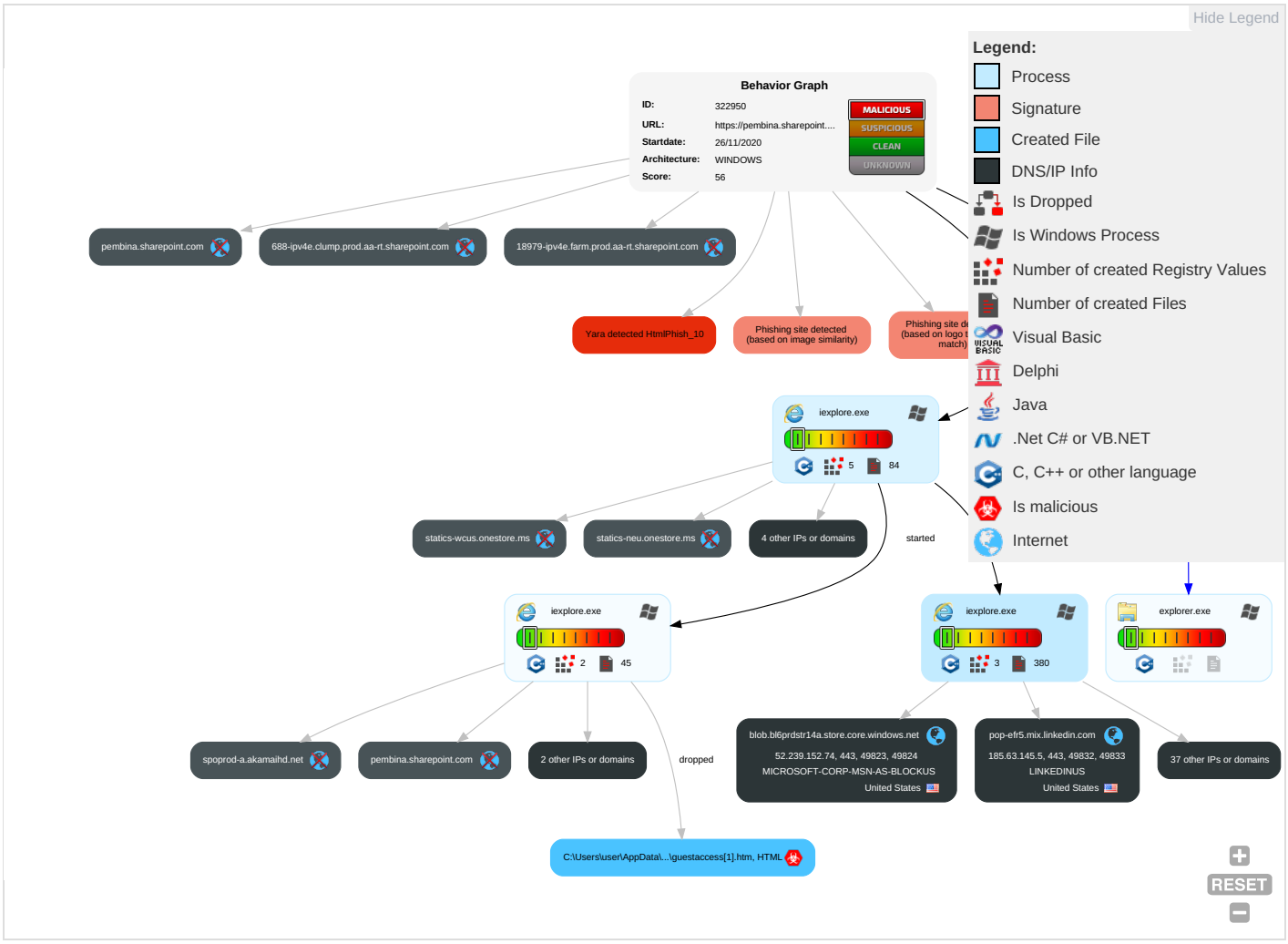
Phishing site detected (based on image similarity)

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	Impact
Valid Accounts	Scripting 1	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

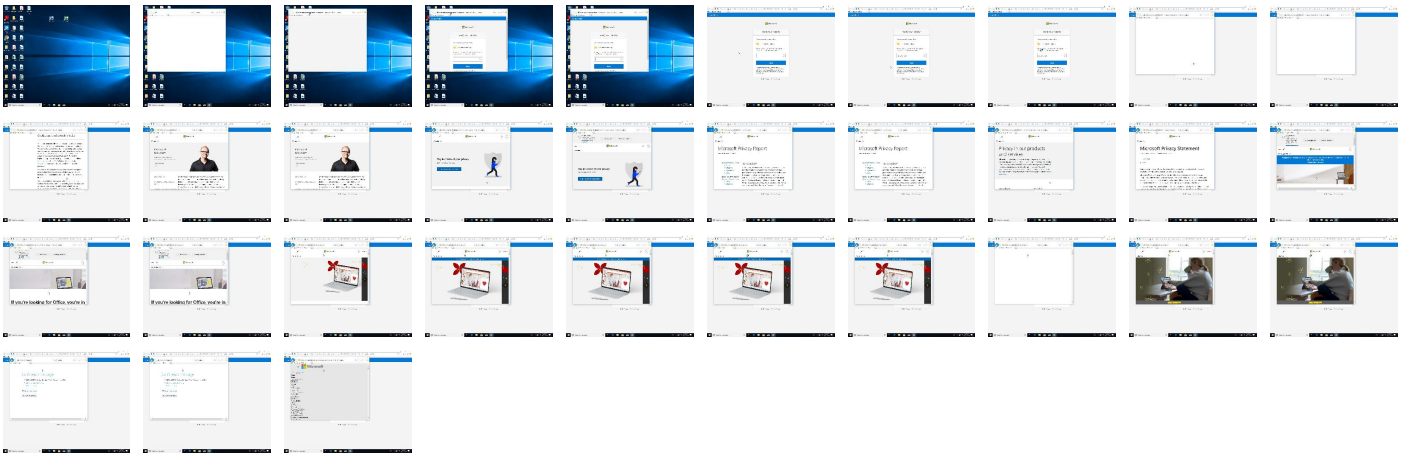
Behavior Graph

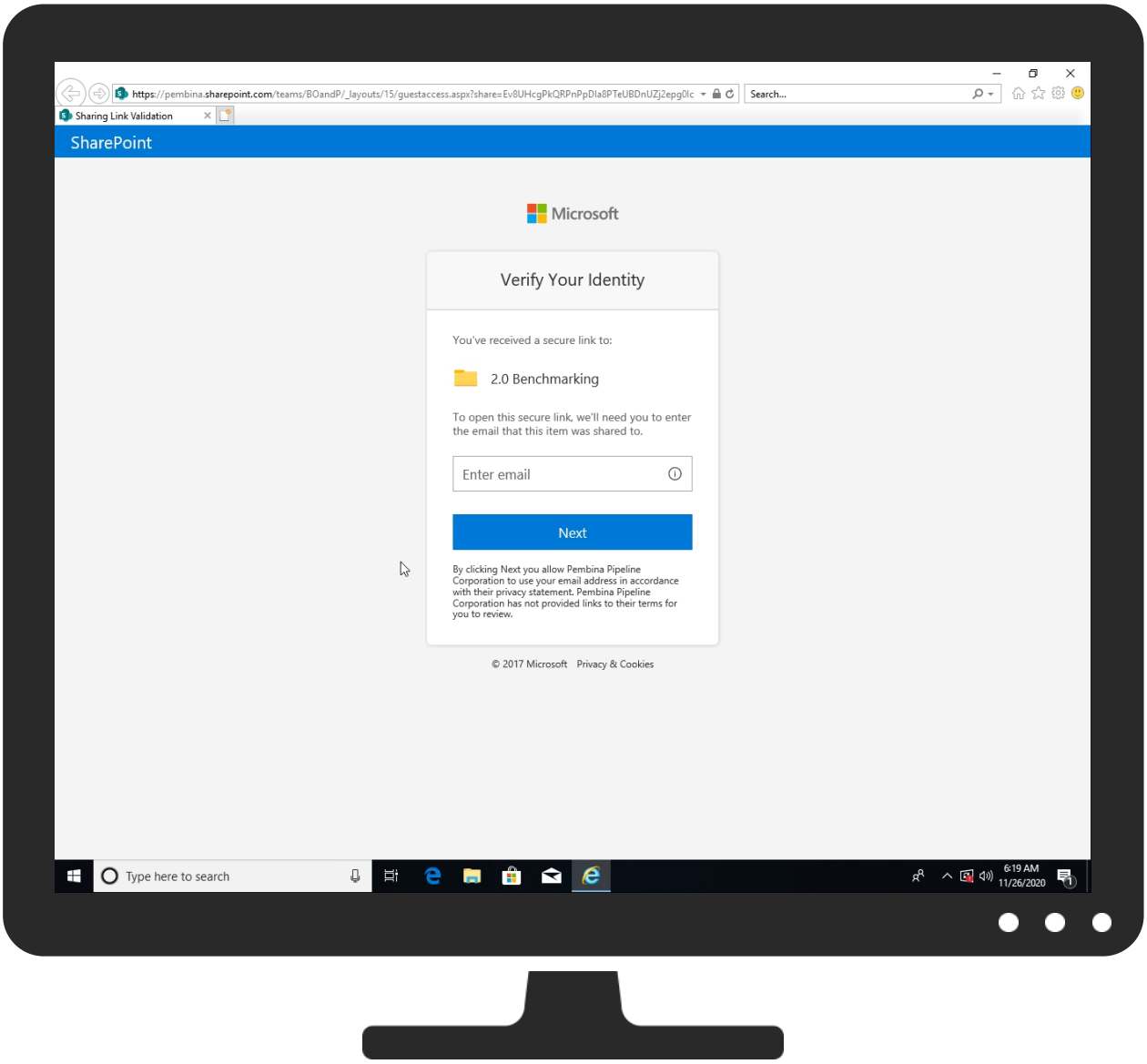


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://pembina.sharepoint.com/teams/BOandP/_layouts/15/guestaccess.aspx?share=Ev8UHcgPkQRPnPpDIa8PTeUBDnUZj2epg0IcLzD6O0XQNQ&e=5:GyiSQ3&at=9	0%	Virustotal		Browse
http://https://pembina.sharepoint.com/teams/BOandP/_layouts/15/guestaccess.aspx?share=Ev8UHcgPkQRPnPpDIa8PTeUBDnUZj2epg0IcLzD6O0XQNQ&e=5:GyiSQ3&at=9	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cs1227.wpc.alphacdn.net	0%	Virustotal		Browse
api.company-target.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://https://a3698060313.cdn.opti	0%	Avira URL Cloud	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://https://assets.onestore.ms	0%	URL Reputation	safe	
http://https://assets.onestore.ms	0%	URL Reputation	safe	
http://https://assets.onestore.ms	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://https://pembina.sharepoint.com/_layouts/15/images/favicon.ico?rev=47	0%	Avira URL Cloud	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://https://privacy.mv	0%	Avira URL Cloud	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://www.michaelbromley.co.uk/blog/193/a-note-on-touch-pointer-events-in-ie11	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://privacy.mcom/en-us/store/b/black-friday?icid=	0%	Avira URL Cloud	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.iask.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	
http://www.kkbox.com.tw/	0%	URL Reputation	safe	
http://www.kkbox.com.tw/	0%	URL Reputation	safe	
http://www.kkbox.com.tw/	0%	URL Reputation	safe	
http://search.goo.ne.jp/favicon.ico	0%	URL Reputation	safe	
http://search.goo.ne.jp/favicon.ico	0%	URL Reputation	safe	
http://search.goo.ne.jp/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/	0%	URL Reputation	safe	
http://www.etmall.com.tw/	0%	URL Reputation	safe	
http://www.etmall.com.tw/	0%	URL Reputation	safe	
http://https://mss7-1.azurewebsites.net/surface-earbuds-b.htm?activetab=overview	0%	Avira URL Cloud	safe	
http://www.amazon.co.uk/	0%	URL Reputation	safe	
http://www.amazon.co.uk/	0%	URL Reputation	safe	
http://www.amazon.co.uk/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/favicon.ico	0%	URL Reputation	safe	
http://www.asharqalawsat.com/favicon.ico	0%	URL Reputation	safe	
http://www.asharqalawsat.com/favicon.ico	0%	URL Reputation	safe	
http://www.movable-type.co.uk/dev/keyboardevent-key-values.html	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms	0%	URL Reputation	safe	
http://https://mem.gfx.ms	0%	URL Reputation	safe	
http://https://mem.gfx.ms	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
scontent.xx.fbcdn.net	185.60.216.19	true	false		high
microsoftwindows.112.2o7.net	35.181.18.61	true	false		high
blob.bl6prdstr14a.store.core.windows.net	52.239.152.74	true	false		high
p13nlog-1106815646.us-east-1.elb.amazonaws.com	50.16.119.144	true	false		high
cs1227.wpc.alphacdn.net	192.229.221.185	true	false	• 0%, Virustotal, Browse	unknown
dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com	34.248.49.247	true	false		high
api.company-target.com	13.224.93.10	true	false	• 0%, Virustotal, Browse	unknown
aka.ms	23.211.149.25	true	false		high
pop-efr5.mix.linkedin.com	185.63.145.5	true	false		high
logincdn.msauth.net	unknown	unknown	false		unknown
statics-eas.onestore.ms	unknown	unknown	false		unknown
assets.onestore.ms	unknown	unknown	false		unknown
ajax.aspnetcdn.com	unknown	unknown	false		high
ct.pinterest.com	unknown	unknown	false		high
surfaceselfserviceoffertool.azurewebsites.net	unknown	unknown	false		unknown
statics-wcus.onestore.ms	unknown	unknown	false		unknown
a3698060313.cdn.optimizely.com	unknown	unknown	false		high
dpm.demdex.net	unknown	unknown	false		high
logx.optimizely.com	unknown	unknown	false		high
consentreceiverfd-prod.azurefd.net	unknown	unknown	false		unknown
assets.adobedtm.com	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
mscom.demdex.net	unknown	unknown	false		high
px.ads.linkedin.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
pembina.sharepoint.com	unknown	unknown	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mem.gfx.ms	unknown	unknown	false		unknown
cdn.optimizely.com	unknown	unknown	false		high
statics-neu.onestore.ms	unknown	unknown	false		unknown
snap.licdn.com	unknown	unknown	false		high
statics-eus.onestore.ms	unknown	unknown	false		unknown
amp.azure.net	unknown	unknown	false		high
spoprod-a.akamaihd.net	unknown	unknown	false		high
offertooldataprod.blob.core.windows.net	unknown	unknown	false		high

URLs from Memory and Binaries

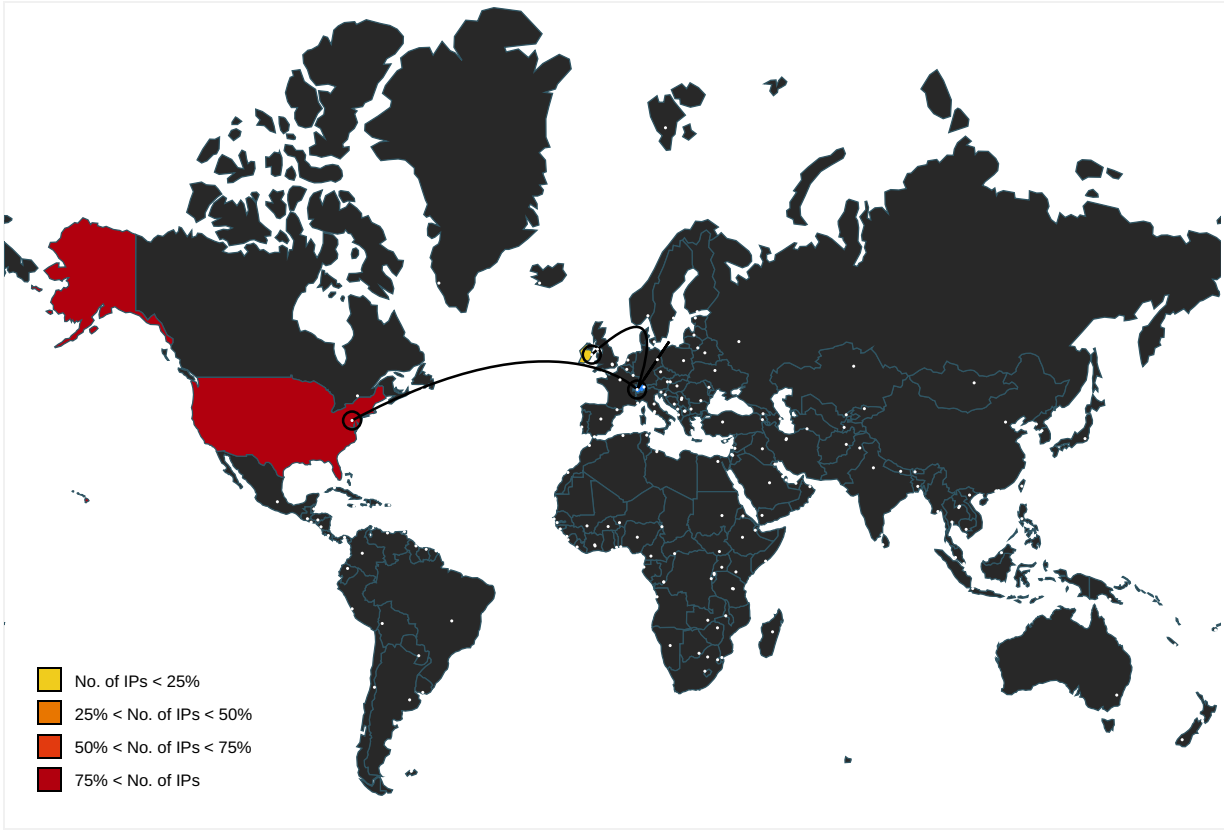
Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://a3698060313.cdn.opti	iexplore.exe, 00000001.0000000 2.840353798.000002A1DE298000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.dailymail.co.uk/	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://assets.onestore.ms	black-friday[1].htm.11.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://codepen.io/tigt/post/optimizing-svgs-in-data-uris	mwf-main.var[1].js.11.dr	false		high
http://www.asp.net/ajaxlibrary/CDN.ashx.	privacy-in-our-products[1].htm.11.dr	false		high
http://www.fontbureau.com/designers	explorer.exe, 00000006.0000000 0.693582939.000000000B976000.0 0000002.00000001.sdmp	false		high
http://fr.search.yahoo.com/	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false		high
http://in.search.yahoo.com/	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false		high
http://https://www.xbox.com/ft-365?rtc=1	iexplore.exe, 00000001.0000000 2.839658795.000002A1DE0B2000.0 0000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000006.0000000 0.693582939.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://msk.afisha.ru/	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false		high
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://pembina.sharepoint.com/_layouts/15/images/favicon.ico?rev=47	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.ya.com/favicon.ico	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.hanafos.com/favicon.ico	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://mscom.demdex.net/dest5.html?d_nsid=0	iexplore.exe, 00000001.00000002.849495516.000002A1E224C000.00000004.00000001.sdmp, iexplore.exe, 00000001.00000002.840092556.000002A1DE14D000.00000004.00000001.sdmp, {F9F12701-2FA6-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false		high
http://https://www.skype.com/en/	black-friday[1].htm.11.dr, microsoft-office[1].htm.11.dr	false		high
http://cgi.search.biglobe.ne.jp/favicon.ico	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://css-tricks.com/probably-dont-base64-svg/	mwf-main.var[1].js.11.dr	false		high
http://search.msn.co.jp/results.aspx?q=	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://buscar.ozu.es/	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false		high
http://www.ask.com/	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false		high
http://https://privacy.mv	iexplore.exe, 00000001.00000002.840520808.000002A1DE300000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.google.it/	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false		high
http://search.auction.co.kr/	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.de/	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false		high
http://sads.myspace.com/	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false		high
http://www.pchome.com.tw/favicon.ico	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false		high
http://https://app.optimizely.com/v2/projects/6249654628/audiences/attributes	6249654628[1].js.11.dr	false		high
http://uk.search.yahoo.com/	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false		high
http://https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/2418adba327c/RC30b69654d14a4895ae64b6e5cf0cf81	RC30b69654d14a4895ae64b6e5cf0cf812-source.min[1].js.11.dr	false		high
http://www.ozu.es/favicon.ico	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false		high
http://www.michaelbromley.co.uk/blog/193/a-note-on-touch-pointer-events-in-ie11	mwf-main.var[1].js.11.dr	false	• Avira URL Cloud: safe	unknown
http://openimage.interpark.com/interpark.ico	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.gmarket.co.kr/	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000006.00000000.693582939.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false		high
http://https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8fea6849a28/RCb931a36f851d412386794b82eefa667	RCb931a36f851d412386794b82eefa6672-source.min[1].js.11.dr	false		high
http://https://support.office.com/en-us/article/accounts-in-office-628ea040-f265-49de-b986-be09c3ebf8a9	microsoft-office[1].htm.11.dr	false		high
http://www.google.si/	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false		high
http://www.soso.com/	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false		high
http://https://support.office.com/en-us/article/OneDrive-Help-5943c2b9-fafc-4cb4-95c0-9cc73fcabb30	black-friday[1].htm.11.dr	false		high
http://https://privacy.mcom/en-us/store/b/black-friday?icid=	{F9F12701-2FA6-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://busca.orange.es/	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false		high
http://www.twitter.com/	iexplore.exe, 00000001.00000002.839658795.000002A1DE0B2000.00000004.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	iexplore.exe, 00000001.00000002.837366907.000002A1DD7D0000.00000002.00000001.sdmp	false		high
http://www.target.com/	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false		high
http://https://account.xbox.com/en-us/mscomhp/onerf/MeSilentPassport	black-friday[1].htm.11.dr	false		high
http://search.orange.co.uk/favicon.ico	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://spoprod-a.akamaihd.net/files/fabric-cdn-prod_20201008.001/assets/item-types/	spoguestaccess-a0017cc2[1].js.2.dr	false		high
http://search.centrum.cz/favicon.ico	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false		high
http://https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8fea6849a28/RCa6da6c2ddf044453bdb4d0b0dafda95	RCa6da6c2ddf044453bdb4d0b0dafda95b-source.min[1].js.11.dr	false		high
http://service2.bfast.com/	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ariadna.elmundo.es/	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false		high
http://www.news.com.au/favicon.ico	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.cdiscount.com/	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false		high
http://www.tiscali.it/favicon.ico	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false		high
http://it.search.yahoo.com/	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false		high
http://www.ceneo.pl/favicon.ico	iexplore.exe, 00000001.00000002.837571028.000002A1DD8C3000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.servicios.clarin.com/	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false		high
http://search.daum.net/favicon.ico	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false		high
http://https://www.xbox.com/F	explorer.exe, 00000006.0000000 2.850272731.0000000006781000.0 0000004.00000001.sdmp	false		high
http:// https://github.com/scottjehl/picturefill/tree/3.0/src/plugins/gecko-picture	script[1].js0.11.dr	false		high
http://www.kkbox.com.tw/	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.goo.ne.jp/favicon.ico	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.msn.com/results.aspx?q=	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false		high
http://list.taobao.com/	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false		high
http://www.nytimes.com/	iexplore.exe, 00000001.0000000 2.839658795.000002A1DE0B2000.0 0000004.00000001.sdmp	false		high
http://www.taobao.com/favicon.ico	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false		high
http://www.etmall.com.tw/	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ie.search.yahoo.com/os?command=	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false		high
http://www.cnet.com/favicon.ico	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false		high
http://www.linternaute.com/favicon.ico	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false		high
http://https://mss7-1.azurewebsites.net/surface-earbuds-b.htm?activetab=overview	6249654628[1].js.11.dr	false	• Avira URL Cloud: safe	unknown
http://www.amazon.co.uk/	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.cdiscount.com/favicon.ico	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false		high
http://www.asharqalawsat.com/favicon.ico	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.fr/	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false		high
http://search.gismeteo.ru/	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false		high
http://www.rtl.de/	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false		high
http://www.movable-type.co.uk/dev/keyboardevent-key-values.html	mwf-main.var[1].js.11.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.xbox.com/ixsurface	iexplore.exe, 00000001.0000000 2.836793833.000002A1DD300000.0 0000004.00000001.sdmp	false		high
http://https://mem.gfx.ms	black-friday[1].htm.11.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.soso.com/favicon.ico	iexplore.exe, 00000001.0000000 2.837571028.000002A1DD8C3000.0 0000002.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.239.152.74	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.50.104.129	unknown	United States		16509	AMAZON-02US	false
50.16.119.144	unknown	United States		14618	AMAZON-AESUS	false
185.63.145.5	unknown	United States		14413	LINKEDINUS	false
34.248.49.247	unknown	United States		16509	AMAZON-02US	false
185.60.216.19	unknown	Ireland		32934	FACEBOOKUS	false
192.229.221.185	unknown	United States		15133	EDGECASTUS	false
13.224.93.10	unknown	United States		16509	AMAZON-02US	false
23.211.149.25	unknown	United States		16625	AKAMAI-ASUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	322950
Start date:	26.11.2020
Start time:	06:18:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://pembina.sharepoint.com/teams/BOandP/_layouts/15/guestaccess.aspx?share=Ev8UHcgPkQRPnPpDIa8PTeUBDnUZj2epg0IcLzD6O0XQNQ&e=5:GyiSQ3&at=9

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:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.phis.win@6/365@33/10
EGA Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://go.microsoft.com/fwlink/?linkid=845480 • Browsing link: https://go.microsoft.com/fwlink/p/?linkid=2126808 • Browsing link: https://go.microsoft.com/fwlink/p/?linkid=2126809 • Browsing link: https://go.microsoft.com/fwlink/p/?linkid=2126907 • Browsing link: https://go.microsoft.com/fwlink/p/?linkid=2126908 • Browsing link: https://go.microsoft.com/fwlink/p/?linkid=2126810 • Browsing link: https://www.microsoft.com/microsoft-365 • Browsing link: https://www.microsoft.com/en-us/microsoft-365/microsoft-office • Browsing link: https://www.microsoft.com/en-us/windows/ • Browsing link: https://www.microsoft.com/en-us/surface • Browsing link: https://www.xbox.com/ • Browsing link: https://www.microsoft.com/en-us/store/b/black-friday?icid= gm_nav_L0_BFdeals
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, dllhost.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 104.43.193.48, 104.83.120.32, 13.107.136.9, 2.20.143.23, 2.20.143.14, 92.122.213.248, 92.122.213.216, 52.147.198.201, 51.104.139.180, 152.199.19.161, 92.122.145.53, 152.199.19.160, 92.122.213.240, 92.122.213.194, 2.20.85.93, 104.83.98.153, 92.122.213.247, 92.122.213.200, 92.122.213.219, 104.83.119.205, 20.190.129.2, 20.190.129.24, 40.126.1.142, 20.190.129.19, 20.190.129.128, 40.126.1.128, 40.126.1.130, 40.126.1.145, 92.122.213.193, 92.122.213.176, 2.21.57.112, 13.107.246.13, 104.83.97.40, 52.155.217.156, 65.55.44.109, 20.54.26.129, 92.122.213.195, 92.122.213.163, 2.21.61.5, 2.20.84.45, 52.142.114.2, 204.79.197.200, 13.107.21.200, 2.20.85.242, 13.107.42.14, 2.20.85.30, 2.20.84.189, 104.83.87.109, 13.66.138.97 • Excluded domains from analysis (whitelisted): assets.onestore.ms.edgekey.net, cn-assets.adobedtm.com.edgekey.net, i.s-microsoft.com.edgekey.net, a1945.g2.akamai.net, l-0005.l-msedge.net, star-azurefd-prod.trafficmanager.net, statics-marketingsites-eus-ms-com.akamaized.net, dual-a-0001.a-msedge.net, account.microsoft.com.edgekey.net, ris-prod.trafficmanager.net, compass-ssl.microsoft.com, lgincdnvzeuno.ec.azureedge.net, assets.onestore.ms.akadns.net, statics.onestore.ms.edgekey.net, skypedataprdcolcus15.cloudapp.net, c-s.cms.ms.akadns.net, ris.api.iris.microsoft.com,

www.pinterest.com.edgekey.net, lgincdn.trafficmanager.net, c.bing.com, cdn.account.microsoft.com.akadns.net, a1531.g2.akamai.net, spoprod-a.akamaihd.net.edgesuite.net, c.s-microsoft.com-c.edgekey.net, compass-ssl.microsoft.com.edgekey.net, 18979-ipv4.farm.prod.aa-rt.sharepoint.com.spo-0004.spo-msedge.net, spo-0004.spo-msedge.net, cs9.wpc.v0cdn.net, a1985.g2.akamai.net, e9412.b.akamaiedge.net, c-bing-com.a-0001.a-msedge.net, compass-ssl.microsoft.com.nsatc.net, i.s-microsoft.com, statica.akamai.odsp.cdn.office.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e9706.dscg.akamaiedge.net, go.microsoft.com, prod-video-cms-rt-microsoft-com.akamaized.net, 2-01-37d2-0018.cdx.cedexis.net, 160c1.wpc.azureedge.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, ie9comview.vo.msecnd.net, cs22.wpc.v0cdn.net, mem.gfx.ms.edgekey.net, login.msa.msidentity.com, skypedataprdcoleus16.cloudapp.net, c.s-microsoft.com, e7808.dscg.akamaiedge.net, wildcard.licdn.com.edgekey.net, waws-prod-mwh-031.cloudapp.net, go.microsoft.com.edgekey.net, a1963.g2.akamai.net, az725175.vo.msecnd.net, cdn.o6.edgekey.net, e13678.dspb.akamaiedge.net, query.prod.cms.rt.microsoft.com, wcpstatic.microsoft.com, mwf-service.akamaized.net, arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, e11290.dspg.akamaiedge.net, www.microsoft.com-c-3.edgekey.net, query.prod.cms.rt.microsoft.com.edgekey.net, login.live.com, e11070.b.akamaiedge.net, watson.telemetry.microsoft.com, 18979-ipv4e.farm.prod.sharepointonline.com.akadns.net, a1778.g2.akamai.net, e10583.dspg.akamaiedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, statica.akamai.odsp.cdn.office.net-c.edgesuite.net, e4343.x.akamaiedge.net, statics-marketingsites-wcus-ms-com.akamaized.net, www.tm.a.prd.aadg.akadns.net, web.vortex.data.trafficmanager.net, e10583.g.akamaiedge.net, t-0003.t-msedge.net, e55.dspb.akamaiedge.net, blobcollector.events.data.trafficmanager.net, privacy.microsoft.com.edgekey.net, e2699.dspg.akamaiedge.net, account.microsoft.com, c-msn-com-nsatc.trafficmanager.net, a1449.dscg2.akamai.net, arc.msn.com, e5048.dsca.akamaiedge.net, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, mscomajax.vo.msecnd.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, e6449.a.akamaiedge.net, www-linkedin-com.l-0005.l-msedge.net, statica.akamai.odsp.cdn.office.net-c.edgesuite.net.globalredir.akadns.net, wildcard.cdn.optimizely.com.edgekey.net, web.vortex.data.microsoft.com, lgincdnvzeuno.azureedge.net, privacy.microsoft.com, e13678.dscg.akamaiedge.net, skypedataprdcolwus16.cloudapp.net, www.microsoft.com, c1.microsoft.com, a1813.dscd.akamai.net

- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.
- Report size getting too big, too many NtWriteFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
06:19:24	API Interceptor	1x Sleep call for process: dllhost.exe modified

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\DOMStore\BACZYXTY\www.microsoft[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1991472
Entropy (8bit):	4.919783139297843
Encrypted:	false
SSDEEP:	24576:r3l3o3o3d3/3S3S3N3x3f3f3T3W3W3z3S3B3B3j3z3z3c3N3v3/3B3+373/3J30P:/
MD5:	4AC85475E508649585CF77CAEFAEFD8D
SHA1:	2C3007017312294DCD6B8D9D1D80BD28604BF161
SHA-256:	3A41B4302DB83AB86A1A6FAE2B74FE5E039DCAC9D3F0C157B7BEE7C07C37B99B
SHA-512:	488A5894ED545510F0A2E521458E97D7C446F0A3B45A26BBA7E91C20B5A1E879776FB2F3170741F3952D9E2C9EF6D2E8EFB93725904F3F04E6B8D7915A663285
Malicious:	false
Reputation:	low
Preview:	<root><item name="com.adobe.reactor.dataElementCookiesMigrated" value="true" ltime="2662831280" htime="30840570" /><item name="ai_session" value="wkalf|1601450621701.26|1601450621701.26" ltime="2691221280" htime="30840570" /><item name="optimizely_data$$oeu1606368018417r0.22586889163181056$$a3698060313$$events" value="null" ltime="3563699376" htime="30852019" /><item name="optimizely_data$$oeu1606368018417r0.22586889163181056$$a3698060313$$event_queue" value="null" ltime="3563699376" htime="30852019" /></root><root><item name="com.adobe.reactor.dataElementCookiesMigrated" value="true" ltime="2662831280" htime="30840570" /><item name="ai_session" value="wkalf|1601450621701.26|1601450621701.26" ltime="2691221280" htime="30840570" /><item name="optimizely_data$$oeu1606368018417r0.22586889163181056$$a3698060313$$events" value="null" ltime="3563699376" htime="30852019" /><item name="optimizely_data$$oeu1606368018417r0.22586889163181056$$a3698060313$$event_queue" value="null" ltime="35636993

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\E5F0NRSV\a3698060313.cdn.optimizely[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	180499
Entropy (8bit):	5.067525848341495

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\E5F0NRSV\a3698060313.cdn.optimizely[1].xml	
Encrypted:	false
SSDEEP:	3072:XssyossyussyGssyussygssy1ssy5ssy+ssy84ssy+ssy82ssy0ssyHussypssy9:3
MD5:	B8340F2501D94720FF3E67B430EE0D33
SHA1:	CC4C46F5E9F3868DE7CC59F39924DC8BCE2A06B8
SHA-256:	34C1FB52F6C5AD1B0AD6DE53B91D23C0A303A86332A6A25261E3F3694F716F17
SHA-512:	16C6591B6427E142A4E6B05DCD12CD7F700E2164DD11C01AB8433A6654E228DCEC16133F58D4374A47785E0B3D87112DD9129992DCEE4D3687AE8578BAC602E
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="https://www.microsoft.com_oeu1606368018417r0.22586889163181056$$a3698060313$$tracker_optimizely" value="{"data":{"account_id":"3698060313","anonymize_ip":true,"client_name":"js","client_version":"0.139.0","project_id":"6249654628","visitors":[{"session_id":"AUTO","visitor_id":"oeu1606368018417r0.22586889163181056","attributes":[{"entity_id":null,"key":"","type":"first_session","value":true},{"entity_id":null,"key":"","type":"browserId","value":"ie"},{"entity_id":null,"key":"","type":"device","value":"desktop"},{"entity_id":null,"key":"","type":"device_type&q

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{E79BECB7-2FA6-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	60616
Entropy (8bit):	2.1249782744071064
Encrypted:	false
SSDEEP:	192:roZjZP229WptyifRl7zMxTB0eZD0Isf0nlijr018R0hi9/qAy/9W09Hy/G0uoy/X:role2U7bk7VE1l9MyF3Jxg
MD5:	50C9514BFE5761380216679FA5FB488A
SHA1:	AA0D6670CABCD28525CA812CBFB2256B5667EB3A
SHA-256:	658112B873F8157647CE8AD50208910F5E839F9452742E0CB7AA18C74221DEB8
SHA-512:	3ECAAD25AAAA7D4A8E6501FA8C01A08B388030821E7C056ED8BA664C252D2E861628496911F349D7558FD83BAC26280ACE76DB3D40ECA81F2F34A0E5BA07A4B3
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\{032EE54B-2FA7-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5659092524222005
Encrypted:	false
SSDEEP:	48:IwaGcpr7GwpaUG4pQsGrapbSftrGQpKjG7HpRltsTGIpG:reZVQk6qBSftFAyTlt4A
MD5:	248BE85C3FA67C9100412451485F0363
SHA1:	4BBBCE529B9106B0C995F0F6CF47F4B1FE3DB3CB
SHA-256:	DDCE475144D4023CED17E80E8CEE8C77CD42E0A1274B4F1488BF0ED08C136FCC
SHA-512:	45B6431F9AC9E06BE85AEE1B0A91C64AA67D054F443A2E3652FC66FA2DE2313DB15B33B575D931DAC4B2EFE69558AD5A45D7A52218BEE59E5CECB2D803189FF6
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\{E79BECB9-2FA6-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30396
Entropy (8bit):	2.262982861615556
Encrypted:	false
SSDEEP:	192:rHZgQI6ykoFjV2IkWEMTYTPvIdmn3JQLwQLMOdx5LSA:r55TrohMMxTWPvGmn3JQlt
MD5:	7B71FF3C3D28495B471533D46B3FAC67
SHA1:	C4946A458D458069E1E11C9F21CF883E537A00BB

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E79BECB9-2FA6-11EB-90EB-ECF4BBEA1588}.dat	
SHA-256:	436746EE26934794FA9072A2271CA711941B83AF6CA2E8D8F5646D8F3A90DE75
SHA-512:	5AAADCEDFE1E5ECC2A34A8F77E07C90FC73CD9A2C5827396E6B08C855E22C1A3177EA3F297DD0C4ACB8ADA5996740CE293C2456B56E1AD87B7825C47CA66E 149
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\{E79BECBA-2FA6-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5829251229484973
Encrypted:	false
SSDEEP:	48:IwsGcpr+GwpajG4pQbGrapbS1rGQpKzAG7HpRhsTGIpX2AGApm:rwZ2QV6PBS1FAzbTh4FPg
MD5:	FF325D8428D44C2A2E01BA13F13E3C8B
SHA1:	0CE063D3C2D13A56801D5CBE19826B4F3B511574
SHA-256:	540EB2F78DF0916DB859448CCA231F54A17041B007C74EBC9D6F6C6DC192A3EA
SHA-512:	62CCF6591322D477D6EA3F5A3142F866FBA2DDE146520A81FE3D8F5EE97508385E98D09B00BE921A6FF519D56EB92F21F03BCBB6DFDB43A1C9053AA90B197DE 6
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\{F9F12701-2FA6-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	214218
Entropy (8bit):	2.7389935275080726
Encrypted:	false
SSDEEP:	3072:01/T0Mz5stOA70zlkl+pRnkdlrPCt+hZMOZMyZMxIIgR:H
MD5:	507D0843D2CB13117E5CB5A201D611ED
SHA1:	6F1CBD4B52B0BA50B226DF2A1D21A20336BC640A
SHA-256:	B2F5EE23D50EBCB300EEE8C6CFDC426E9CFFA9AC8857D77CA218E82A276E4509
SHA-512:	8362456212F63386E6F096C0CFA79E35666A17F7E8F470C9762EB81B5A7D9BC81CD82819C469AA986AC31A00AF81E5A615BA72408638E2D61B01F47AF4B8E6F1
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.072314610731222
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEBnWiml002EtM3MHdNMNxOEBnWiml00OYGVbkEtMb:2d6NxOoSZHKd6NxOoSZ7YLb
MD5:	59E53AD5B8862D692C5F1C3DA6BA24C6
SHA1:	BB2F32C7A4717309F990A5C9BFBC332B324C49AA
SHA-256:	045746526CC9A5C0D758B4EAE31086F327BDBAA6CDA14B8D9BFAC06B1A8B69BF
SHA-512:	CB62EC6C2DE2DCD26CA31BD9027F6EA500A262076BC17B87B29137F258F5C0A8154142CA2F534F1C38D8F890B361C2D7E5D0DDEDECB578619AEFC221FB612 A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xbe5f39fa,0x01d6c3b3</date><accdate>0xbe5f39fa,0x01d6c3b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xbe5f39fa,0x01d6c3b3</date><accdate>0xbe5f39fa,0x01d6c3b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.102146048196839
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2k9nWimI002EtM3MHdNMNxe2kd4nWimI00OYGkak6EtMb:2d6NxrISZHKd6Nxru4SZ7Yza7b
MD5:	7FB740398A66A79558204FEF387C79C7
SHA1:	647DD31B631FBAD86A46C85C9B0CD3A13D629D55
SHA-256:	A8ADDC92F68F58CA0CBE7181B7286D275004D9E71BF6448E2A270D0E541C3718
SHA-512:	027A238D5A1B963A6FC52592CA7CB4F119706B030B86A66A187A2F2AC98A7E6BB96CA6E613AC452BE696F695FE0C55C2A1A6CD894D057B69CBDDEC852831798
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xbe4e89ea,0x01d6c3b3</date><accdate>0xbe4e89ea,0x01d6c3b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xbe4e89ea,0x01d6c3b3</date><accdate>0xbe50ec17,0x01d6c3b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.096847905098487
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLWJzJGnWimI002EtM3MHdNMNxvLWJzJGnWimI00OYGmZEtMb:2d6Nxv3SZHKd6Nxv3SZ7Yjb
MD5:	F63BE91767BE5FCCD851AEFAE962DF4C
SHA1:	738C2671DD349B470FC1826A125C9FA06E2C7DC9
SHA-256:	611B3B717B389095F6CC91699A6300FDC64C9446F061BD011EE81E2F50CDFAB0
SHA-512:	48323CFFD2D239D1EF487300C15E8A32F44ABBA684BC8E779FB3A81E06A7797E35CDEB67E0BDAF5DC8B7C35B0A55E7168FC8EF012BC011B95AC08F4C33D51298
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xbe619c51,0x01d6c3b3</date><accdate>0xbe619c51,0x01d6c3b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xbe619c51,0x01d6c3b3</date><accdate>0xbe619c51,0x01d6c3b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.0750371438877115
Encrypted:	false
SSDEEP:	12:TMHdNMNxiggggbnWimI002EtM3MHdNMNxiggggbnWimI00OYGd5EtMb:2d6Nx4FbSZHKd6Nx4FbSZ7YEjb
MD5:	D06B356353EC75B761C22F7903B2DDC8
SHA1:	A5F0961E7880E4301EE0C1499D520B0A0AEAFBDC
SHA-256:	AAA7454F96E5246C1B9F999CFADF405F892DE3E99EA4A53036850B97092FA65E
SHA-512:	008CEC097618651919F76CD4A0CC31FD9502E179FC730F6DA83D242777630DE0B3F56685C590CC3A24AB33EA1E5FA15ADD197BF749BB98A1AF2CD56E4A12943
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xbe5a7530,0x01d6c3b3</date><accdate>0xbe5a7530,0x01d6c3b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xbe5a7530,0x01d6c3b3</date><accdate>0xbe5a7530,0x01d6c3b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.10467425005523
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwWJzJGnWimI002EtM3MHdNMNxhGwWJzJGnWimI00OYG8K075EtMb:2d6NxQ+SZHKd6NxQ+SZ7YrKajb
MD5:	F4510CFE44C4FEA268916819A796CD70
SHA1:	04A2FF25354805CE057DBBDC8D8E4179E0690E23
SHA-256:	A8495CE6B30D5F4F655907A82E0690B4EC57865D9DCE0780F39079232C49DC39
SHA-512:	ABDD1747AC34E952DCE9EDC8414E4D5374EE71B7203668C1566655CC45C9FE5DC01D40524CCC9A3A0FF8FFF2A816C9E03F7A29698EB8248DBA3DC92FC12039
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xbe619c51,0x01d6c3b3</date><accdate>0xbe619c51,0x01d6c3b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xbe619c51,0x01d6c3b3</date><accdate>0xbe619c51,0x01d6c3b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.075977536366461
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nBnWimI002EtM3MHdNMNx0nBnWimI00OYGxEtMb:2d6Nx0BSZHKd6Nx0BSZ7Ygb
MD5:	7C761A99CC9DD160DA741AB6B09C27BC
SHA1:	462F28BB65D9A50B101084D85461FDD7760A37EC
SHA-256:	EC00892A60B5CCE1259A0161223CD8E7EDDEB252204CEA82E5C2EC281F0C5DB4
SHA-512:	CF77EABBB159184F5E4EAF0090C300F810CE4DA17240EC741802794BCEC6ADD5FBD7057A40EE8BC83FDD23ED57F2B9686649219 41B8017E8E71AE3A9BCF6759
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xbe5f39fa,0x01d6c3b3</date><accdate>0xbe5f39fa,0x01d6c3b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xbe5f39fa,0x01d6c3b3</date><accdate>0xbe5f39fa,0x01d6c3b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.101140291657264
Encrypted:	false
SSDEEP:	12:TMHdNMNxx1nWimI002EtM3MHdNMNxx1nWimI00OYG6Kq5EtMb:2d6Nx3SZHKd6Nx3SZ7Yhb
MD5:	CDD3E4DDE887CF81F51C7040321E72E0
SHA1:	8928D94252330E353C7B1B4B4C88395170CD6551
SHA-256:	121DE5D7AEFE8BEA6827F259B6E4F2C933EDAF4FC3186245171996E855D3CEB6
SHA-512:	76FCCC4D3A5647EC98873FFB19A58E0457872C9EA05AA865BC6E39343024C56460B472B03322605F3C2952D9D5282D54B6098288050A79C1BEA2C254AD49C67E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xbe5cd78c,0x01d6c3b3</date><accdate>0xbe5cd78c,0x01d6c3b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xbe5cd78c,0x01d6c3b3</date><accdate>0xbe5cd78c,0x01d6c3b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Entropy (8bit):	5.093675263457104
Encrypted:	false
SSDEEP:	12:TMHdNMNxcfWunWimI002EtM3MHdNMNxcfWunWimI00OYGVEtMb:2d6NxGWuSZHKd6NxGWuSZ7Ykb
MD5:	A36EB5AA321E0C3D8AD83D25FC520A71
SHA1:	3B7FC90981A9F17109EFABC91A31BDC9F9D04990
SHA-256:	0FC51F87C114778CE902836E805C25BDCE1411D0108D4CE92211F082AB328852
SHA-512:	8157ECF74293C6ACF4BA2A0A6879C08E1973640FE74B3D55DF3F4FA30F6685900EAC1B3F10205D77455E319DA89E535139B6FE8D0F70C1C2B7954363960A5DFC
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xbe55b095,0x01d6c3b3</date><accdate>0xbe55b095,0x01d6c3b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xbe55b095,0x01d6c3b3</date><accdate>0xbe55b095,0x01d6c3b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.09015408231088
Encrypted:	false
SSDEEP:	12:TMHdNMNxfngfrfgnWimI002EtM3MHdNMNxfngfDgbnWimI00OYGe5EtMb:2d6Nx4jISZHKd6Nx4UbSZ7YLjb
MD5:	E63522F40EBDCDA18C9AFF401DF43ECC
SHA1:	4D395E85C03ECAF96D0DB5745470454F298C8573
SHA-256:	7E2CA54829836B722AE96BC16609FBCC225E65AB1B022B286D5895B1E7A3A873
SHA-512:	46425E548BBDB90BA0661EC431573DB8A0C5007EB8AB0986523A0E090CDC5249369B39120F50579F8A0E6048F9B481C5C339973EE1601AE3727F154146E23825
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xbe5812d5,0x01d6c3b3</date><accdate>0xbe5812d5,0x01d6c3b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xbe5812d5,0x01d6c3b3</date><accdate>0xbe5a7530,0x01d6c3b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	53748
Entropy (8bit):	3.0427782100502307
Encrypted:	false
SSDEEP:	48:bAJbAybAybAGgyyyyyyyyyyyyycbA0XbA9QQQQQVi6b6W6O6tgyyyyyyyyyyyyyg:CQQQQQMQQQQQAQQQQQB
MD5:	F09614037F1CADA91DAAD57581DAB72C
SHA1:	43CDD7A522AF3D70800122323684344E12017A5D
SHA-256:	F716FB14E41DE307D2C37DEE060FD4849E4B0E5B383F8BE55B234692D0A9509B
SHA-512:	68B1ECDF6DB8A5CAC1725C53A7FB8DC4336ACD321962CAD017334EB80468DB6F5727A25943071F69E0C4E090A5E13E6DB1335F45C044863E21299C6285743B7
Malicious:	false
Reputation:	low
Preview:	(.h.t.t.p.s.:././.w.w.w...m.i.c.r.o.s.o.f.t...c.o.m./.f.a.v.i.c.o.n...i.c.o.?.v.2.~(...............h(......(...................(.................................."P......................................."""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1083_Panel01_FullBleedHero_BlackFriday[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 1083x609, frames 3
Category:	downloaded
Size (bytes):	150886
Entropy (8bit):	7.93436592054122
Encrypted:	false
SSDEEP:	3072:es7jbcZfwKcA/7G3kjqN581Skl+ftLBPpqS0ycPuVhmUHMja7t:e8baYKckK0jY5M+fjsSh5jt
MD5:	C992F4DA540E6877C45298301DCBCFBD
SHA1:	446F30ABFACF0BDB947815E6804B34EEF37C75C0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1083_Panel01_FullBleedHero_BlackFriday[1].jpg	
SHA-256:	44FFDA0EB54552C04A39B1ACFAA4926672E6D8047ACB25F621CC79865CF77CFB
SHA-512:	21D93029863E96B8DAC62A45F00FA0AC12DFE0D43CEFCC4427ACE0FDACDF40FD4CF63221CB8EFB943C36B8EEED5A7670032CA4703ABB61A11A10CDAC5253949
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1083_Panel01_FullBleedHero_BlackFriday.jpg?version=49313388-fd35-56ba-a074-925298cce7e9
Preview:	......Exif..II*.....Ducky.....Z.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 6.0-c002 79.164352, 2020/01/30-15:50:38 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:DAD270CD0ABE11EB9263FED807190012" xmpMM:InstanceID="xmp.iid:DAD270CC0ABE11EB9263FED807190012" xmp:CreatorTool="Adobe Photoshop 2020 Macintosh"> <xmpMM:DerivedFrom stRef:instanceID="B704B954EFBA65C9097D7DB5B6B9EF9C" stRef:documentID="B704B954EFBA65C9097D7DB5B6B9EF9C"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1083_Panel04_FeatureGroup_Need[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 1083x609, frames 3
Category:	downloaded
Size (bytes):	228028
Entropy (8bit):	7.982439965505789
Encrypted:	false
SSDEEP:	6144:aqbFGp4/QSVCPRyWaIU5YuqoH6A3c/hEPThiikbDYO2U:aqbF7HVCZpU5RPcGPTp2D92U
MD5:	36EB2E4866A82DDC9CCB4C15D1A4CE1C
SHA1:	766412A78E7B16C953FACA207CC01011355E4404
SHA-256:	8536B31B32FA0B78FB51DFFCB4D3B82FB06C0B74BF943A163DB8E0E4A350A2FA
SHA-512:	72323BF138ACA9E5AC571F99F60D3CF47B537EFF22601C0264CF0C724A16A2D13621882110006 48ED5EE42964B5488263298431 16A542D11BAADF68CAB23F97B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1083_Panel04_FeatureGroup_Need.jpg?version=91703ef5-c3b8-2d66-a08c-97c99700ca58
Preview:	......Exif..II*.....Ducky.....J.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:E9A5235D5CD811EA88EEDBD181122FD0" xmpMM:InstanceID="xmp.iid:E9A5235C5CD811EA88EEDBD181122FD0" xmp:CreatorTool="Adobe Photoshop 2020 Macintosh"> <xmpMM:DerivedFrom stRef:instanceID="849B4255D84E95FCDEAD1A88F392308E" stRef:documentID="849B4255D84E95FCDEAD1A88F392308E"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1083_Panel05_SneakCarousel_Persona1[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, 555x369, frames 3
Category:	downloaded
Size (bytes):	63799
Entropy (8bit):	7.988404642427592
Encrypted:	false
SSDEEP:	1536:ai/KhiHhSo06gSOCnGbVVJE+QcIoOnK0Tcsp:ai/jBSd5CnGBVJLQhKscsp
MD5:	98F03214917680B2B0E7DBD7169AA311
SHA1:	98DD8D1A159EAD606C414AABF06451D7C2981F30
SHA-256:	066486E3F8794C8438457545BDC5B01116713F4E2B52FAEE437DAF1E57ECB74B
SHA-512:	1DDDCE64AE7883C2567F7C252BD64D14118733FF16E7B20EC1D638AFBC2C6AA10349D6A85470727838DAFBE9321890F67DE8CDBAD54B0F9E20840065E307010
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1083_Panel05_SneakCarousel_Persona1.jpg?version=666dfba8-769e-481a-66af-cb0be6ff8823
Preview:	......JFIF.....q.+.....%.....*..!-.;...i~..iT....= .)=.,...b....>.@.`?Y.~...8.....s..=.u3q.^a.M.....c3w.....F.4'"%....".r....JhZq.....].x.s..i.{R....<.j$.[;.m$|F...H...a.....b6.P..+V.s.....w..I..9....F:...e...G{:....$.k..&.(.....B.\A.5..n. .6....,w...5..[q.~...8.....\u...!..S.....K.b.bD1..#*.-..4...+.....r.G.'.....P.B>]D....-.M.O..$N.....$...1PD....i...UR../z.3....X>..hM..Q..6..26.....P^.;.tU.....n3.I.x.@...R..Ns...M.. .&bQ.w..xFk..?...t"(....6.XP@...:...,k.>}...7.x$.K aN.....Y..u.....RH....sB.v..9.....J.Sd7.R....Z;..]...k....S-.1.nsoJaK...J...Ek.k.Z.....zT..kT...3D.JH.&'F>..%..S3....f.kOn.j.!X ..C7."D.v...CkA...()....R.y.#..*..R..s...}.s.*J.s.~L...L.....k.w..Mx.....&...s[wj.....JR.. ....\.....I.G.*...G"Z..{..#'...*.a...Wki.j.=...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1083_Panel06_FeatureGroup_Gaming[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, 1083x609, frames 3
Category:	downloaded
Size (bytes):	259454
Entropy (8bit):	**7.991415388003182**
Encrypted:	**true**
SSDEEP:	6144:13hnkt5PdPEVzehHrZT4+q97yuuOCWmF/8uA5zz:nnkgqHR9Gb79mFEuoz
MD5:	B8F0D4F6E846F168B83C83E26B92E873

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1083_Panel06_FeatureGroup_Gaming[1].jpg	
SHA1:	083F8E22959D0D9A22BB45D0EA8E641BE77A94EF
SHA-256:	BF77A38A3560CB4F13CC945B923E2C31B6B47B015296E1819CB29CD8F4A1C007
SHA-512:	3FB240AC5C766B7BC622DB388C3197F8DC43F93ECB2A8103E6357ECD65F4752CB7E8B98B787C7A0A87618A39594242C281DBA8353C09AB15230D86398A092F3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1083_Panel06_FeatureGroup_Gaming.jpg?version=21b8d32f-c6c6-aef3-5a17-1179fd22d7f4
Preview:	......JFIF.....a.;.....*N.I<.0..v.D.5!...j..k.....O.Q... .OLF...fi.....S'iz]7uQ.yU*.7.O....T.....m...#...0Wem...vl.-.....h...A.pl.}P.X.1'...*."n..O|".....Y$L.6`....._Q..%.....F5Z'. .....C|Y.2N.J.;:...>....lp..OF:.Q.|.m.z8.O.....b.\...(. ...9sB:s:N.T.%w...%7.y.P.a.9;.<..v{4.....h[..'V<.G:..b...t.%].....D.A`.f.(Q. f..Lz.'.6....a.....&.M...)..Y.....<e..H.....e.G..''..C.j..E8.s.).....[T..%tVN.....dO.....N.=1.....q V...D.w^u....J.W+...Z..W..m\'.5.....K..@.?B.{....X)~a8_....x....z.!.....~.r...<.5~...M.....V.y.2X.~\3rS.J..p..V:X..'.z.!..=.'.....!f.9-.N`pH...=:....Vd\.....>...W..P.~z@g.H}...[.qe....V. ..... |.....(Y..;V.BE..56D....nP.6..\....(<K!..*._J.\Da.....Z..G.../.p....P:.f.y....|<.*.Go...C.p....r..Y..i.;?..k*.....x....G55.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1083_Panel08_MultiFeature_Learning[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, 1083x609, frames 3
Category:	downloaded
Size (bytes):	109655
Entropy (8bit):	7.981060947881193
Encrypted:	false
SSDEEP:	1536:7WJ/tfTuiOlC75cL7nXYVjWilp1054o5RiPOnLNLs+ou4nA3p1p9hEEnJnzzNyUq:7+Ap+054SwPSL9sJu4nA3p1p9TtNyTZ
MD5:	E408A41D916B5852E7C0F69E98DDF2BE
SHA1:	9089AFFE45C9C359E61F2C178DA0D3AF4704E88B
SHA-256:	F2BC868AB50093DB4E5F17A2691CBCDAE779D47A7FB81674230DA70A21B02D7D
SHA-512:	57FACE0D80DDF374BF1F937EDD315B7265DF9292083357AF8F2EED12F6E7EFE5E4CBC57732F107668FDF8740C43406513427EE1C682874A0E66DF0AB86FB9E2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1083_Panel08_MultiFeature_Learning.jpg?version=e677e1ed-830e-f88a-633c-dc048f3ec5bf
Preview:	......JFIF.....a.;.....U.....I.c..1.....A$.(.QI".H..I RvM....9.C.J...\|....\.w.y./...p..4....3.q.....c..;.i.yNcg..r/Z.{....}..@..k.....h...I$...@..E..A.\..%M.,.Q]Cpp._?D.z+.Q.O..O.y...'.9.=.....;.V.M.h....e.T.6;Z.'.:..m..!.bc...&.4...@j...)..!8$. I../....N^...[.....\...[<.[..7...e...9.-.^...}.Ya....mIW..j....B.....5..M...h...A.JI$.I".!._...?.Z...x..9{..S....O...,.d..7^.?.x.....S..{.sKc.7M..q_wF.W.z.....4...`c.....D..I$.D.....*uM. x.Zz.&.L..C.4..}.....A.=/...c.q.k.....QT.7.E.....<..;.w.....M.....1.....cCSZ..$.I$.(..I?S.\.....)..&k.pI.^...b..+.tjO.~..f.-...:...MQ...w...G(..I.~...^..e.[..$....`kZ.....kZ... .I..A..E.i.!.W!q. <.....<.....?.P.Zo...}=..3E.f.zJ..6_-.O.z".....g..\....m.....51...kZ.....h.. Z.D .D..F..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1083_Panel08_MultiFeature_Mobility[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, 1083x609, frames 3
Category:	downloaded
Size (bytes):	124609
Entropy (8bit):	7.984861343519558
Encrypted:	false
SSDEEP:	3072:XJzUyEhXXbcQuEkEWTLNGrc1wbUDI/POljWDXQUWbeTi5nz:XJzhEZbDd0kc1ps38jutWbeTihz
MD5:	779FFDBE0434CE42273C8C5807A7BEC0
SHA1:	19A07B1E5B79085D2EF7A9FD71CABB5EFE8DB8C9
SHA-256:	E06838AEB7EC1445331BA4782615E85A6FAF116D715908D5E45F09465086FF66
SHA-512:	6A3F2EC2AE1341CF6B0235D1E723CCA795E913A7B762E82F36F88A8440DBCBB9E37BEE0C04402372CFD7E1107F869FB8003683325092F68B85A285B8081F0B5D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1083_Panel08_MultiFeature_Mobility.jpg?version=c0ecdb42-f74b-56ec-d258-d462bd483d36
Preview:	......JFIF.....a.;.....2..Eh...^KQ%.z).k...C...!.o3333 333337.....T8..nY..2...N[/^..gLV.35.....fk3Y...f.Y...5..N..e1X..I.....?..c.....n,=K.....ffffj...\s..d.Ral..A...../.fk333Y...fk5....f.3Z.fk5IT..Lv.(..j...Q.....5.&J.....ffffB...^}.l.. 8..7..%.%m....m.3335...ff...#3y...I..{.....u.xuW.Pc.S.....K1c...V.333z.....f.z..@..W.....5...c.5.....}.....5..#{.f'y.J7..3%<.C.....w..}<.331.!....fffffffffff.3332.... Q..z+.....5....f..... ..:J...ZF..i..e1R...<U.....Lzw.....''<...6S.....ffff'....*S.7]...q..H..N...c.....Z.y...4.P...4.P..V...].>.P.....:..9..N..R....@...S]V.333333y.....=t..wP..[X.....''<..I.....zK-i.W..k11..e ;.R.,.1.&$w%?..Rt..%.....|.:Y.j..1.p.....{.....ffoY....`..x...Wc.E1P.!....M#g.....E'',.^.!..kzj,..T./.}va..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1083_Panel08_MultiFeature_Neurodiversity[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, 1083x609, frames 3
Category:	downloaded
Size (bytes):	182272
Entropy (8bit):	7.976051301297215
Encrypted:	false
SSDEEP:	3072:ttfC2ZL6JHIbDC+dpQoHRNW5eUITtFJkUYmVefmwhqUjD3L0PD:/fPZLMHIPVdpJHR6e3PkUxEe+qWDIPD
MD5:	2CB81F3882ABA9A8A1092BC6A63ADB1A
SHA1:	39FF0D2AED9EE5BC2C09B048BCF27732D81FA8D9
SHA-256:	7FFD74BE52D35F8517E9FA91D10E51728602947AFCD48C51A12EDD72E8D5B547

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1083_Panel08_MultiFeature_Neurodiversity[1].jpg	
SHA-512:	1A6511E62697793AF200027615CE7EBC21924D107911EDBD3B61123C58E6082317C842C8864230ADF772F9696064A02C605476DA37104089FFE12789C26FE96F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1083_Panel08_MultiFeature_Neurodiversity.jpg?version=e062b307-0a98-61bc-3662-5d94c74c1206
Preview:	......JFIF.....a.;.....y#..Ya..&Oa.....!.Q...../.*,1... <H...W..$..|.Sf@.y..j.R.V..I...m:..".B...*J...Et...]z.3s12..AjL...d....k.3..G...".A.3.....^/W..}.D...}.).'...._.?...R+%`.X)I.%HRP...O.g.>.mt...O..6.>u:..x.nO..../G...H.H...0Q.O.'..Y{.l@... ..DC.E~..U.^...@.....B.u..W...LUea.....h.d.....W.~..D~..X!.b...>,/.I..K....Y.2mT..."|..DH..zT...V.BV.....V.-i..{..g.Q..\P.Seb...S....n..I.....m.Ea6\.Y..y..'...L.....D.B.b..E{..o'*.*.U-U.. .....W...\&'.. +.....&...o.o..+.e.....Y..mg.bDmH..K&V..h..h[*..L.V.T.*.M..Qj...%H..yJMz.ak....}..Kb..!$3.....9>.....Z.YI....99.._T.W.E.V.zk....(...V.>H*.eR..$.hB.d.HJ... ..-.>..p... ".YMX...4..c.[m.5.'...Y.#`..YZ.xz=c.g..Z.IYH.,6.{">T..k.J....X!*..EU.....Hx}.....`Qil.(.l<.....#.W.r.E.....6..p.4Ru...xn,,V.Uz.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1083_Panel15_Mosaic_Item5_Stand[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, 542x400, frames 3
Category:	downloaded
Size (bytes):	16475
Entropy (8bit):	7.814365220066478
Encrypted:	false
SSDEEP:	384:fbZaAb0yUMZ95IQRVAfobZCXLd/ZIFNHNY9tFiINeFwsQqH9:DZgySQjBShANa9tFiINe+sQw
MD5:	A2AA2B4620EC4C797042811C008D3B89
SHA1:	B23CE846CC395867F219C33C42A094197816B9A6
SHA-256:	FBCE541750335AE8C5BB4839F2D7EBCFC7B5224E0CE01B97C17EE89E6ACBBC80
SHA-512:	34B8032574C430C5639BAB431DA8BDEAD67819666728173787D4BBD3DFE6C9A48EE6F21172EDAC5D0C7B46455BE6954A82E9BFC996126922DC2854129D3741D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1083_Panel15_Mosaic_Item5_Stand.jpg?version=00530597-9619-2575-35f4-6d87092a5ab8
Preview:	......JFIF.....!.GS:-.zi.Q...vi....T.EB*.E[..|7 ....a..@...+.H.V.+.....AC.f....PT..aR.-.W...@..1~h.....U...3.=.nN...c.....".XT.po$6..zO.!.+..8.....`(T...rO_y.T."..3....QR*.TB+....]...".R...8...X"..V.*..g...*EJ1.f...V.H.EJ..w....=.. .T.8.Y.....*V<..?w.;.T."....T*V.*U..._....8T....?.@..V.H.+....._>..V..X.2...X....D".l.k..k.AR*....2...."..(T...=..z.....1.c...."..+..W.....v@*V..F:.@..T"..".Q].....i..Ua.1.b..V. ..*T.t....l. ".TT.c....X..*.a...*..Q.:..T.Pc<...T..T..!.t..<{.,.D".aP1.f....DT..TU.<..G..U.+..W...."..".V...A...^.n...U...?.....B..a...9..j.n..]..XEQ..8.G."".....a.V..o].g..S./au.!.D.*p....."...W.y...#. .R7>...../.....EH.T..L!.=UU....U...p.....!.+.7.....Tu.{..U.....9t.....a.....v+...~t.3T@..X.Yt....EH....t./w.;,".P..a..T+...D@"...T.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1920_Panel08_MultiFeature_Mobility[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, 1600x600, frames 3
Category:	downloaded
Size (bytes):	164044
Entropy (8bit):	7.9854058825476475
Encrypted:	false
SSDEEP:	3072:PTt3xNdtSq6s/zGCBKRtX3AshnVxXJyUx2Uf4jzLz+JvQfLstsMDkweWRMjyOmS9:PTffY+ojhnV3y82UfKHPZ+MLm6
MD5:	9C30CB9B4D52B8B57B260421BB813452
SHA1:	481E44056B658635D5F2122112637DF9616C54D7
SHA-256:	AD094954A7FFAF116311CB233FD50C5A9859A6ED43BF20D5CF5C564E1E0725DF
SHA-512:	C4D91EEF1F967F0BE228C0C254101E9FD04EF504ED754E750E6DA0D92FFCB06EA8FE16DE7CE54A2AA422738DE1BD9A7A441DC4D5C4947F1EAB2577DB6508D 41
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel08_MultiFeature_Mobility.jpg?version=d6cee281-0b4a-7da7-45c1-9290b6842199
Preview:	......JFIF.....X.@.....y-d.`.;...$.P.u.(H....^....~....>.. U@`..l....9.}.{....{.....g....b..k.F .T...L....P...$...M./~..3.c@kU...*...aP.T5.^....|....8.M.Y_.G..i.N.6.....3.B..[{n...Q.Zr...=de*.NI.iw.WCp}....F...P.18.-..9z^...{.....3.c8.=.{.... ...~..%.!...z5..r.r.....U.N...._z..xpU ...Ln.}.b4..ZC.....~.....B.h.r.1.G.eh.l.J..l.l.l.C..:g!...6..G..:.K..(.?Wtg'./{..c...j`..e9...}.g8.1.g9.....={....&..}.H.V.<1q7F.k....Lz.\.)...t.....^.V.Oh.`6. N8.i.f.../)..F.....dm..z..he..q.R*.b=tm..^FH.....p.W.0..1.}.(uZ...p.~..n."^.....Z..{.3.'+...^.}.G..e.{..}.{.....Y... .Wc..E.8..{.Y)D..s.6..n.0.4.&fl..;.euc....m/%6ef0.Z.<.W&.....R.. ..?.....:.&.l..]4.S...wL..^...N.....?g..".@3=.....y..b8..g....{...|c.v.W..+..*.1.W.<.E.|g1..Q`..M..?..._.:cB...~cDk.ral(..Q.../.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1920_Panel10_4Up_Ideas[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, 358x201, frames 3
Category:	downloaded
Size (bytes):	26797
Entropy (8bit):	7.9702343818998465
Encrypted:	false
SSDEEP:	768:j9g2HNjMjNt7tf5xAqTKQQWyLCEmAeUU13:xaBNVoQN1XAeUU13
MD5:	7F13D5037F3845E797123874BCC2122F
SHA1:	FE8E8EA5160C7D4EC61EBB8B0ABCE3157565D8A8
SHA-256:	93ED25E616450B512FC1038805238C83669D1006CA7B3FBEC2A811DCDA05211A
SHA-512:	F18F05318C805DE99EED7839856981A5A22C366102B19F498CC210CE71896C75855B77B5B528811D2169C51AA2AED3EB1C6CEBF7504E1089DAA282FD1231385
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1920_Panel10_4Up_Ideas[1].jpg	
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel10_4Up_Ideas.jpg?version=4aa4ad31-1581-9d76-ef2f-e9ebe3f8e42c
Preview:	......JFIF.....f.....k...b.r.....~]@.*....:.c.....C.I ....teso..D..3..*M.....'6..&._v$X.krX.=kt'[.B.....z....X[.n.6..F.?.k....@..ip.k.d.....&./..... .j`...K.....^.....&...y.....Ix.....^.y.z...x.....5.5.w.mL...p.N...l..>.g.....|..].....u.....].g 9.....k...d.\,N..j`...F...".K_]..63...&..|._B%.v..S.....(I.....%.m.0....kc.....S....,hr.-...f.o...u...F.FyR.=.....#.;..|...i.t...#n..g.4FWf...E..^N.....*."..Z...]3+OO9o.+.m..+b..M.....+.- t.....yz....)FyqpX.L5tw....n...`..F.6...7X..~...+.k..P#T.....6.....u.....r}..>Sjt..u.%%._.....1..&..z.i.....\...t.4.|.....M.]".R...oru0.....f...r.....k..Ws...lru0..uk...8e.p.....6..B6...ru0..m.... ._.....M.W..t....L..uk.'.u.+....I._...:..y:.....y'.}....!.....*P.m...8...2.....z

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1920_Panel10_4Up_Protect[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, 358x201, frames 3
Category:	downloaded
Size (bytes):	29147
Entropy (8bit):	7.961451918944927
Encrypted:	false
SSDEEP:	384:fnD50xW1Fc6TjXDSEenJQU4pAAEKFizUBFJV6x+ii6ypj3v+sLP2sTUbHOxUos4U:OonjXDSfF4c7IBFixypjosQbHOSQHWSo
MD5:	0B2DA7A96DC4CC1893336F3D6D9C0F87
SHA1:	ABB5F097A6DAA9344761E57EFC48F74F69E03B5A
SHA-256:	336E770A9E30DFD7ABEAAFC8A2BACC166E85EBA6F0BC17FB95A6EC8BD1AC9FBB
SHA-512:	C38BD88D2302D28FFD502F84E1CFF4DB94D1320A6199561C9C28465D9A545B91A7AEAE1E501931DFBF6CF9E46C1CF16B5354ED75FA68EA94F25FCE34D60FA8 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel10_4Up_Protect.jpg?version=74ddf6ec-e0f2-b1c0-68de-ae8073b23695
Preview:	......JFIF.....f.....2.....-.vqX..3...p.....<. ....~..$.I6n.....\.zG0..p.i.....{.O....[.....q..W.g.t&.....X..u.bM...F9W..l.z.$.....&....`....u..~9...7t..k.O..=.E*Q..f.\....(....j_r...m.o...xL..B....2.4..t.mR..mH.e`.'9.n...:... r=.q.V.pH^8.P.....W....VV(.....i.f.>C..z.G5sE.aNd.O1.|.n.ca..7....w.Iow..^5Ro.UW.)....Yh.Rp.G..m.....Eg..Oi....:%,.^.....Q.....=.g<..~{B>....._....%..Rn.r..q...su.....y..gPF/.- .;...F2O..}B...{.Q...R.zE.W^....W.....)....&.U.xm..W..IE..'.....*Em.;+.=.,.....u.Q.t..Wz].g....2.Yy.r.Ug..D-~.y.....nW.v.-..ru6..4....k.!.RmJ.+..eZ3E..^*Emt..1...g..,.z..F..k....b. .j.su[3....3?...H.....%.V3US[9..v.|.Ij.....z..5%.%(....:.u...|..[JW...M.).m.....F<IK..Y...=*.iMH..7..L.....IZ...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1920_Panel10_4Up_Time[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, 358x201, frames 3
Category:	downloaded
Size (bytes):	24781
Entropy (8bit):	7.959533628424081
Encrypted:	false
SSDEEP:	384:fFKoQhDLqNNTgWscFsy33ldqJJvxAdSdwp55uDOZekhJwnQ8K2LIMsgECAB1XlUo:PQhyNznHdSdYYcPz2LIMsZXXuEF
MD5:	192C75B0EC4A529EAC5AA62048D14D88
SHA1:	1625492ADBE68315E1A436F4176AE56D2466F01F
SHA-256:	F8C279C2FF71AEBE12722C6A6DD0CE2CAF1E2B988CB4CE9FC1E8124DBC3077E3
SHA-512:	04558F9178311E29FC6C0677F5F28CF13516A3F32FE4A11F5F2B7A50BC15DE4F3C3F3F433D2E5267AC3D18363243975C42942A496B31102E6EDBC9F1729799FC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel10_4Up_Time.jpg?version=5b146a03-52cf-74f5-064d-eee060433c0b
Preview:	......JFIF.....f.....s.a]...Kw...5.8 ..O.....Kx..Vr.+..~. s...[tb....\.&6.<.KS5....v...F..Y....).3..ZcfR...b....f{\..=j6_.3R...r.Gd[...D.a..=.zt...o..+f.OF.....1....].....}y._K.k....W.F.&6.F....9t..W.....M....~{I.....Y.....n.....].N.....k..... ...y._K.b.A...9.-..w..B.S.V..#vf..t.,....j..'.Q.....#.@.`r.].Q....t..+C.h.<{.\.....\l..<.....W..8.-.Y.a...Z...5.>...a...`k.P.$F_K.[..4.[6.S.e..X.{.F..lPY}.*R..}..n.c..s...2w.f=.6.,....j.m.....]. ..!.x..{.n.,b^.a.....I!ki..].vw.>.7B...@.D..'u...N...K...8....`;"W..).-.[....-..C.0.z0.9Sa.}...<._^.rd.....Z.W.~F.#.8.e.ng...|..8l.....T..&7K.....E..,.[...Ng.kS..I..U..Zf]...s}..p.>....[O....6..=. e.a...o.1..~$b..d]....H.,lx+<..\<;..e.....1.9.T..QB.p.....&..F.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1920_Panel10_4Up_Together[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, 358x201, frames 3
Category:	downloaded
Size (bytes):	21386
Entropy (8bit):	7.958734469990998
Encrypted:	false
SSDEEP:	384:fUQgNVMRBiYcHKCwVGzH2ble7bJhq1Q43IS4uo9u341zQs5eKQl3ugh:LyclYcqRVQWB4bLKQDSiuIJQqeKie4
MD5:	D3434A3C6938E1D1D157B3729C9E1E0D
SHA1:	A98ED69CC59566FADD550F484BF75715D93C8841
SHA-256:	C611FB750B26CDDAA8D48EF46AB4F9444898F9728D1364A398EAEC852A19C3D6
SHA-512:	1A5078D17A9ABEFC480937C3E036CC74F8CF2F352C56EFB41CAEB50603EA43B3806D2A24451912BEA3A432A9CCD96F20B2E9BF82D2260C3C33228C9470BF0F5 E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1920_Panel10_4Up_Together[1].jpg	
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel10_4Up_Together.jpg?version=f129679d-4e30-ff68-4e6f-246b4b6387be
Preview:	......JFIF.....f.....mB....m..YW. .....r.....X.[....| .0..z..R.kU.\..Z..DI...@+.*.....kj?lH.?.O...96.T.F.o.HS.s..07..."..UF5..(P....$`..... ....(..}co...,~...k..=...z.. ....(..T/....@.uZ.....%.....s2 .J..Z.%H.N..'..}#...;.H\(.Y;..K....s2 .J.....:~r.. ...5.\|.....U.@#...2P..U./....k.n.^.n....w.J....fD..B..%.PIz$.F..u.U3.....K..i.u.@#...E....=..L.h.*7I]C.(..|...9?I9....@#...C8V.....B{.!.....u.@..;..quR).....fD..."Ko.Nx.\.d....])).R.T. .S.=..Y!.....A..n.(..?.t+oI..,4..zl.^..H...G3"..p.|.L.....Mg@uL.....q1.Q./n..Z.. ...!.%bv....f.uA.J....9.....#.._..9...k..D.=.5m.7...w....d.5K.....d.>(.....^T.....N^..a.;.L.p..`<.],.J.. ...*..}..}i.F~e5K{~.S#... |..o.a....gtW...fD.W|...'T...ME...7.<.?.~.N.).....y..6..njm..m..=.C.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1920_Panel11_HighlightFeature_Apps[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, 1600x600, frames 3
Category:	downloaded
Size (bytes):	144467
Entropy (8bit):	7.957330768323046
Encrypted:	false
SSDEEP:	3072:SGnPI8T8ArCgtlqqWvCnTFNjHwKxXGOSjPKi9Yn2kN8c/9m3w3lDvlBa6:S9831zf8CnTrrwr1y2kSQrlDPl
MD5:	27EAA6A3D5F234341A7956081B790398
SHA1:	86A929097F2A414369A4E028D250456C6DF71B96
SHA-256:	FCC0A06617B5E1EB631F16478A334B5E8404AD63A5AA4F4AEF3264A75071C012
SHA-512:	ECB62F5362638B231FDE4E7EA6BB54D05513FD4D0E8174CBA8F0A54F344F73DDA8E3514C5C496EC248DE501F4244015FAA75D8CAB2DC680147F659A37D4E6C 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel11_HighlightFeature_Apps.jpg?version=20838ec0-a03c-6daf-0748-1ae153da306c
Preview:	......JFIF.....X.@.....f.. (.b.>h.M.....g.@5_SKI. .....)...ir_4k.....W?...e=.;]'\....;..k...l.I4/.zG.c....Pe..SRR./2.....#r.w....u.}..H.*T..I.!.T....d.v.S.....@.....K}.r5]=%7x.@...,_....<..>...V~7.).yMa.F}#....z{..\....1..s..u).....t.5.@....- .y.w).8..<..&D..."L.6.v..R.J..b=*T....%F.E.....ia....G.....'.....i.....n.././]...i...Z.".C_....."..R..O ....^o...b...>..$....}.Z.Y:.C.<.\..2.f..k..5..]O.....*}7W.T...~.^G.....= D....o..o.|q.....Vp.9...78[.C.T...y.I.../g(.1.=..j).)|....~..W.8...?"D./.}..vM.....e.....{&.@....!s.....[.\V.X.P....aUSQ.....E.>.._g..=....'9.....^..zR.y.s~....).....N.\`...x..\q.y .."L...}..z...r...PV.w=....MK.q.....,0.....i....]'..ZyN...}....TRR.}../-xo...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1920_Panel13_2Up_Home[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, 740x417, frames 3
Category:	downloaded
Size (bytes):	93919
Entropy (8bit):	7.983580727472191
Encrypted:	false
SSDEEP:	1536:Jmx2U1Y3Ax/pYPcDHUeC6i6gbmlhSFabuXv+6tqXyBDkrN/sOIE5H:JA1Yo/SxeCr6wmHlb6TcXyNkrNb/F
MD5:	454AA79511263AAFC09A5D1B55BD09E0
SHA1:	C15C6416DCE500963D977E46175952AFE2235A28
SHA-256:	DBD9E0D003B7F50C04DFC6D8A77CA221CC58E045F854154765D5339034143DF5
SHA-512:	8D4D7E204EEBC550FF4271BCDF3F47147604436F7CFA6A79980A0C84C816FC9FFE93A369AE608A952E96F0BF4E1E82AFB88BF1D1BFB2359975F76A8B0BE1335
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel13_2Up_Home.jpg?version=eac57ec1-493d-31c9-6134-0f496332edfd
Preview:	......JFIF.....wwq."c.D.=....].l.1..#.#.....N ...!C."..A.#..U..y-Q5..:..P.....p..7.{.....0..p...wp....^..H.....FAf..n;..o.`..!....8....W.o.t..+...#. =..<=.....p..H...m.n.7....wZ.[...ww....."#]..]&EM..s.1.TL&.....(.....~C. .....P.....1.F...h..'....fpJ.!.!...<<!...../.JP..9...v1...:..p...@.....<&....WBY..,.^...{i.....n.../.C..N..8{.....4.....s.U..C..xL"_;..IFo.?X.<QV....U.L=.=....#..^.....p.`"!{D.. .K...}..op ..pwp....C..^Gf.9E.g....z.B.a.....JB...I..}..H.m.\oYe...< .....=N.....Q....~n....~..X.L...<...<=.....!8LD._>O.1.y.a...sZo.....;..xq....$...I.f~.i..i/.a.....@.T.&.l....w..... .t..rW.$.f_:Z.j.....O4/V\....x....MP..p....wp..p...8.@.J.t..q.q...=z...OB!.....&...JK.W....zG.Z....f..3..?O..@.n.....3Y

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1920_Panel13_2Up_Pro[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, 740x417, frames 3
Category:	downloaded
Size (bytes):	74824
Entropy (8bit):	7.989036787290381
Encrypted:	false
SSDEEP:	1536:hFTY36SMcXTIWbnwKZd0BOFpuo9Ke5U6pM5FG4nTzyMUxh:hlEXJwKZdcOPiQUoM5FXnaMKh
MD5:	DFBC329C921F5BE1FD6DA59568C8797A
SHA1:	0C15A6297043096812FBE0F5D89623536F6D2AF0
SHA-256:	12D81261AB70A8FF51F76757193EB1632A2FE34368824155DF12C9469000F285
SHA-512:	C62336A60CD723B920D65664683E60237C42CF145DAD4BFD14B355CEDF863333DBDD9012BF72E1B37B8238AC658A50741DD45895F0661B1FA7254AFF80076B5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel13_2Up_Pro.jpg?version=6254e865-59d9-772e-b366-18c5a317c764

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1920_Panel13_2Up_Pro[1].jpg	
Preview:	.....JFIF.....DHV.....}..._P..x.j.....[..(S....|.n.....kaX.*.+U....y.Pq...QY..F.a.=,1y.X.:4iT!..\..crf.:/H>.X4.....r.'..%.&s&6.....(t9.!+...q...E.v..q.....tB.(...Z.i."J...uzZQ%&.....=..*^..L.y..G...h)...N|..\.\.]....q..,.n..].`..3fS..B.jj.].0.....C.....ME...V*I)<%.J.<.....ph....S.Q.w&.r.9i....w..C.2..._.....:..L.....\.J$I..sI.#...Jdw.v.Q.kD..#N..z.....Mm.Id2a.....n...C.....C@mA....f.i..Y.E.....z.k.5h...g...7.ap.T%....:i..Y...^....,(.{;.J..`q.1..A..b6.....Gm-..Pa...4....'J.%\..<....-.....xs.j~$....s....4..2._...N..{.pJL.....R.{,.....#-R....(k.\tf..B.#I[.m9j....1.....FPK..b..B)#(.j&.e.....o.~..../.;.~.Q>.k..xW....)8J,.8.]A.M..4.B4ik.m.+R0{.OJd..I..MQ.HID.....\.....1.....jl...,...9..r!..%../.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1920_Panel15_Mosaic_Item1_Gray[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 890x400, frames 3
Category:	downloaded
Size (bytes):	15776
Entropy (8bit):	7.430669868094102
Encrypted:	false
SSDEEP:	384:wy93GvSFm2UHh+sfD0CHb3AEUTyeMcn/pVuc0JlmwW:wCGvSF6JfD0CHbwEUTyeMc/pkc0Hm
MD5:	18745574B82CD2657FE5469381124E0F
SHA1:	F90EE5A06FFB4446A173E33C9958839CA642FB82
SHA-256:	B550A20C433EA98D69FC606003183CF0CBDD955DC0B9C9AF59BF3E3F6B60AAC8
SHA-512:	1BC4B696957D81BF560FEA88E45EB47240824A8A58CB70F2D9A4610B4DD00CDFB2D9F03CBBCDEE54D9FC5370BD35CD3090473F211C0C0257A7BFBBC1ECAC9233
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel15_Mosaic_Item1_Gray.jpg?version=df68d82a-b81b-b310-e0da-f49a63a83107
Preview:	.....Exif..II*.....Ducky.....K.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:A67AEAFA5CB911EA88EEDBD181122FD0" xmpMM:InstanceID="xmp.iid:A67AEAF95CB911EA88EEDBD181122FD0" xmp:CreatorTool="Adobe Photoshop 2020 Macintosh"> <xmpMM:DerivedFrom stRef:instanceID="8F6B98E30D2E75BCEAE1C4EA6B2EEB5C" stRef:documentID="8F6B98E30D2E75BCEAE1C4EA6B2EEB5C"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1x1clear[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.122191481864228
Encrypted:	false
SSDEEP:	3:CUTxls/1h/:7lU/
MD5:	F8614595FBA50D96389708A4135776E4
SHA1:	D456164972B508172CEE9D1CC06D1EA35CA15C21
SHA-256:	7122DE322879A654121EA250AEAC94BD9993F914909F786C98988ADBD0A25D5D
SHA-512:	299A7712B27C726C681E42A8246F8116205133DBE15D549F8419049DF3FCFDAB143E9A29212A2615F73E31A1EF34D1F6CE0EC093ECEAD037083FA40A075819D2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/_h/9be151e5/coreui.statics/images/1x1clear.gif
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\7d-3b8b80[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	168619
Entropy (8bit):	5.044040083782762
Encrypted:	false
SSDEEP:	3072:OzCPZkTP3bDLH0tfRqQ0xtLfj4ZDSIpTt813viY8R1j35Ap7LQZLPPJH7PAbOCx8:clZAXLkeeds
MD5:	7A091EA3F595695C19CED8B52228FF48
SHA1:	587B8C1FFF5C84755C8BE6C2029FC0B46C0F76B3
SHA-256:	C55B3700FA0698B9F057F40512CFD3B9D6AED620598BACE734338F4F6DAF7A86
SHA-512:	522DC920EDA85D8C7F6FA56E959552C477133E1C5C39939331962A221E5C5AEAEC0643FE8F6AFF4384125B4B58E3930751A21CEB7C60C309AD037ED12865AF8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-wcus-prod/west-european/shell/_scrf/css/themes=default.device=uplevel_web_pc/4a-f2fa13/d2-97697e/15-b02cf6/8d-8de298/30-e5ac82/cd-1bda0a/e7-838d86/7d-3b8b80?ver=2.0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\7d-3b8b80[1].css	
Preview:	@charset "UTF-8";./*! | Copyright 2017 Microsoft Corporation | This software is based on or incorporates material from the files listed below (collectively, "Third Party Code"). Microsoft is not the original author of the Third Party Code. The original copyright notice and the license under which Microsoft received Third Party Code are set forth below together with the full text of such license. Such notices and license are provided solely for your information. Microsoft, not the third party, licenses this Third P arty Code to you under the terms in which you received the Microsoft software or the services, unless Microsoft clearly states that such Microsoft terms do NOT apply for a particular Third Party Code. Unless applicable law gives you more rights, Microsoft reserves all other rights not expressly granted under such agreement(s), whether by implication, estoppel or otherwise.*/./*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */.body{margin:0}.context-uh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\7d-3b8b80[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	233703
Entropy (8bit):	5.072962778083855
Encrypted:	false
SSDEEP:	3072:wYzddg8HPbn/hL4fbv3DlF+EkyfJY6F0AJL55gGHjkzmfeT5gbORtJ4J0ZRV8+uv:aLkeedPZlHFW
MD5:	F0B63713AB85463AD11C6606AEEBCCC6
SHA1:	C48ECCD9F5CBD2E9B36440A3DB138029F5F1A159
SHA-256:	CF473DB1259780C028216A14C2DF281C437949ED2922B1EAC4B9B39D8825727D
SHA-512:	D28748E1A51BE8E60C7E80DD361C36E2BE96FFB8D32820B5E2E302977669CDA233F10564ADE0C584E563008ADAE6B39372BB1AB195A77040D59CCAFD3F74B5C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/west-european/MICROSOFT-365/_scrf/css/themes=default.device=uplevel_web_pc_ie/e7-838d86/e2-cfdce6/e5-1b8a4f/fb-45bb20/ea-3648a0/98-bd0547/bf-66bfa7/d3-e247b7/d6-2c2a80/21-7d6c87/c7-542157/c3-953460/8f-a30304/90-c01110/bf-60f63e/81-8ca29e/c0-379397/fd-9178b9/7d-3b8b80?ver=2.0
Preview:	@charset "UTF-8";.x-hidden-none-mobile-vp{display:none !important}@media screen and (-ms-high-contrast:active){.c-uhfh button,.c-uhfh .glyph-shopping-cart,.c-me .msame_Header{border:none !important}.c-logo{margin-right:1px;border:none !important;outline:none !important}.c-logo.c-cat-logo:focus>span:before,.c-logo.c-cat-logo:hover>span:before{background:WindowText}.c-uhf-nav-link{border:none !important}.c-uhf-nav-link:hover{text-decoration:underline !important}#search{backgrou nd:Window;color:WindowText}#search span{vertical-align:top}.c-uhfh.c-sgl-stck .c-uhf-menu button:focus,.c-uhfh.c-sgl-stck .c-uhf-menu a:focus,.c-uhfh.c-sgl-stck .c-uhf-na v-link:focus,.c-uhfh.c-sgl-stck .c-logo.c-sgl-stk-uhfLogo:focus,.c-uhfh.c-sgl-stck .c-logo.c-cat-logo:focus,.c-uhfh.c-sgl-stck .c-search #search:focus,.c-uhfh.c-sgl-stck .glyph-shopping-cart:focus,.c-uhfh.c-sgl-stck .glyph-global-nav-button:focus,.c-uhfh.c-sgl-stck .glyph-shopping-bag:focus{outline:2px solid WindowText !important}.c-uhfh.c-sgl-stck

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Blog-high-contrast[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 20 x 20, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	266
Entropy (8bit):	6.6809756954998365
Encrypted:	false
SSDEEP:	6:6v/lhPUVLlzlr2dmq1whm8pnqWZZgPdXRiPHalM0QUuA3jP8/qp:6v/7aTr2dmq1wU4nqWZZUg6l0ATP8/A
MD5:	A1F53DE45A191696D9552CF7D0C2BB94
SHA1:	B1DD334DAAB4744B3EDC9503DF1F4BE3DDDEA84A
SHA-256:	8A56B4D7E088C0A978E014D429D3952584EDAFA49A6B6ECF3F1E1EF23486B469
SHA-512:	12921A8EF29F333B693C97316027AA43AA234D077B15BBDA1452ECBEC9EE5949F2D5FE7AD89558BBF96B70DBCCEE61F82B0F84A9C408B353488CCD9595B68F45
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/_h/fa221510/office.testdrive/images/social/Blog-high-contrast.png
Preview:	.PNG.....IHDR.....pHYs...n...n.#.>.....IDAT8.....0...W...@F..l"#..l"#8.#..g..s.-..4...G.....`Pf..N..L...w.^.LD..LQ.c..I.}....b...v...0...%....X.X....X..`I.%..}.....i..._b.i...i.5..7t...WS8...sF....:zJ.W.....x....'G.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Blog[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 20 x 20, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1131
Entropy (8bit):	6.4661643982206325
Encrypted:	false
SSDEEP:	24:E1hxWwjx82lY2T3dVafXcyJ3VcgGuAkmPHqlc8r:K6Nn2xUJ3lNAkmPql1r
MD5:	33305B0D90662F816FFF068E3688A4DB
SHA1:	6F30AD31DA07FAACA2D2BD67D8189F6C36E816CA
SHA-256:	207F50299063FBB1F3B17BC02663CC5E8FB3B385E8EA29919D1AF13A7BAA6247
SHA-512:	D9B9B0807B8FC500F50C419C007B16579B43DE316C26C398FDA8406404192F9068F21523BD088524203E36C749D516C5B8FE99F83746D3C1C5EF216D2BD58EE7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/_h/36ff46b6/office.testdrive/images/social/Blog.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Blog[1].png	
Preview:	.PNG........IHDR.....................tEXtSoftware.Adobe ImageReadyq.e<...(iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c140 79.160451, 2017/05/06-01:08:21 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC 2018 (Macintosh)" xmpMM:InstanceID="xmp.iid:D15367BA690311E8A2BCC45AE44EDC95" xmpMM:DocumentID="xmp.did:D15367BB690311E8A2BCC45AE44EDC95"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:D15367B8690311E8A2BCC45AE44EDC95" stRef:documentID="xmp.did:D15367B9690311E8A2BCC45AE44EDC95"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>&Jy)....IDATx....0...6.'w.l.....c.Fg_!.g.:::9.c.APj.r.....6.q.._..\.K....F. ..c+t....a%.A..@'..'C......9....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/ErrorPageTemplate.css
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_gradient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...background-color: #F4F4F4;..}.. ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\MS-Execs-2015-07-Nadella-Satya-24-2[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 799 x 532, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	364559
Entropy (8bit):	7.985439976531035
Encrypted:	false
SSDEEP:	6144:6/nuJ2eZXp8OjVeEdITlsGHNjh99kV++ztjkoeBcxtFvOUcVgEo996/I/:suJZZXSK3ImwNBa++zXvx/GgNZ/
MD5:	6B79DCA87C4B7796A73A6BBC5D9583AE
SHA1:	82E4133376B208DB5F7F7029B63E9CBDAE5AE0F9
SHA-256:	7E453099D8FD62936873D71F8B755FB4F930007B8050DE2950C7EAB700620C86
SHA-512:	A6FC03300DBFFCE0E14DC0EAF9DDAE75120B3235334B7A9F1FD0FCC07E0ADC8F5178C3984231D8481C4BC6B5A759E429581B723BD70920A6D25C8834BD55B0D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/MS-Execs-2015-07-Nadella-Satya-24-2.png?version=1df74ca3-80d7-9ffe-593c-05292a3f8f87
Preview:	.PNG........IHDR.............{..... .IDATx...Y...Y....z...a....G=hl.&$YX..0...Uv.Tl..*_.B.*.r.'.C....@.c.H....-$K......hIt..O.>.>{X.;..\...C...t...S...9......y...?..Q.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ.EQ..#.....|.}i.s.!.>...%....w.i.....&.....(! .|.......z.. .J...(..B.\......).G9._...H.h.....t.#.4..k..QX..I. %...Z.Q.....=..F...!.M"`Y......`.@)M".m.. K..{.R `].$..j..Q.m.V........:G.....n...-..8k1R...=&.l....<...q.3....!. ...DJ.sx.......(.X...h...-M.iaH.@"8:Y...NS.2.]6...D....JpHDp....M....s[9{j.... ..B..."......(..........8.;;.M.....mo1J.5..@h.j.f<*......f!.@0..dfx..;.]k1B...Z.rUaRM>.!..n.!)%u.b....F.1U.*....aF9.B.<..IF.BH..l.k2.H..V..zD.X..I.....(r...../......~.FT+z.Q...$x..R.u..iI..u..<.t....,..^......lV-:.h.p....J#MJ[m.{..g.|kwGZ.Fz'.T.m-J......B...`...Y

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\NewErrorPageTemplate[1]	
Reputation:	low
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RC021d0a1582e845158b9974bf66e669fd-source.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	6317
Entropy (8bit):	5.352229146241528
Encrypted:	false
SSDEEP:	192:0BIXy8Jt0lbHKl6Hr8P/enHIAXecIcm2cxqytkE:0aH6lbHKl6Hr8P/YIAXecIcexqytkE
MD5:	A58D2E1B2946C48052F8EBAB711D04F8
SHA1:	0E38AC84B21A826792974D3023D46FBC68A30A42
SHA-256:	79B4CBB8FD08466802D5A63842ED964C4A814031082606697179 79E7336DDD6D
SHA-512:	A59602144201EF9524B49964E26D2789A375B2C53C824F3CA573CB760884E52619F68889F01384872C269F0DA045BD2641D9EC31ADD6D2CBB5A2D0F2D6421797
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RC021d0a1582e845158b9974bf66e669fd-source.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RC021d0a1582e845158b9974bf66e669fd-source.js`.._satellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RC021d0a1582e845158b9974bf66e669fd-source.min.js', "location.pathname.match(/\\/surface\\/devices\\/help-me-choose\\/?/gi)&&null!==window.wdgtagging&&null!==window.wdgtagging.jsll&&(window.wdgtagging.data=window.wdgtagging.data||{},function(t,e,a,i,N){jQuery(\"META[name='awa-pageType']\").length<1&&i.setMetaTag(\"awa-pageType\",\"HMC-page\"),(a=a||{}).sdata=a.sdata||{};var T=a.sdata;T.pageName=t.getData(\"gpn\"),T.scnName=\"hmc\",T.started=!1,T.qOrder=T.qOrder||{divQuestionFirst:\"1\",divQuestion2:\"2\",divQuestion3:\"3\",divQuestion4:\"4\",divQuestion5:\"5\",divQuestion6:\"6\",divQuestion7:\"7\"},T.questions={};var q=T.questions;N(\".questions-panel .surface-hmc-qa-block-item\").each(function(){var t=\"q\"+T.qOrder[N(this).attr(\"id\")];q[t]=\"\"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RC05ac5f311ffd4e5c9ad450f46819401c-source.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2300
Entropy (8bit):	5.345646088282328
Encrypted:	false
SSDEEP:	48:DG/pt/BuG/Enc/+kJnITzR2rXBtYXc/Cf1wNQoRRvGBf1eSkbJ:6xBBRAoAUI9KPB
MD5:	B2EAF9DE2C6C457BB9D7CB7CB2BA533C
SHA1:	47B430777301755F968066F33AE7138FFFBE3358
SHA-256:	1CD6AC4A3A7300E14F6D32B2ECD7B6A5C43E8A8FA7AB078048B0813AE499F3B5
SHA-512:	999D1BCC03FFAE0138B2D31BF0E18844D27ABBEEE85F87702EE647DE89695E5C75B0597617A74DB6C0B69029400BEBE4A3707A5F53B2BF447B19B9328AC7BF36
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RC05ac5f311ffd4e5c9ad450f46819401c-source.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RC05ac5f311ffd4e5c9ad450f46819401c-source.js`.._satellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RC05ac5f311ffd4e5c9ad450f46819401c-source.min.js', "null!=window.wdgtagging&&null!=window.wdgtagging.jsll&&function(a,c,e){0<e(\"#primaryArea[data-m]\").length?(e(document).on(\"mousedown\",\"#WF-Modal a[href], #WF-Modal button\",function(){try{var a=e(this),t=a.parents(\"#WF-Modal\"),d=a.parents(\"#WF-Modal-1\");c.checkFixDataM(a),c.checkFixDataM(d),c.checkFixDataM(t);var o=JSON.parse(a.attr(\"data-m\")),i=JSON.parse(t.attr(\"data-m\")),n=JSON.parse(d.attr(\"data-m\"));o.aN=\"body\",a.is(\"button\")&&a.hasClass(\"glyph-cancel\")?o.id=\"WF-Modal-close-icon\":o.id=a.attr(\"id\"),i.cN=\"mainContent\",i.id=t.attr(\"id\"),n.cN=\"modal\",n.id=d.attr(\"id\"),a.attr(\"data-m\",JSON.stringify(o)),t.attr(\"data-m\",JSON.stringify(i)),d.attr({\"data-m\":JSO

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RC278c787435b94d148603e89a80d2b336-source.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1136
Entropy (8bit):	5.37516968084438
Encrypted:	false
SSDEEP:	24:DJNSct/BuJNUbElAh33YxsA9fi5a+1QPRuJjeRxa3wuKIPn/:DL5t/BuLUg6gfWavOdr
MD5:	249675EAAA42B635A3C79E1ABDFAA915
SHA1:	C203E3EFA48C0F2209FD472020ECD9B2D8171D31
SHA-256:	919F61BDC0A6CEACE57280C96C107F30EBCD9AE51081CF367FFF9A51C44F6339

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RC278c787435b94d148603e89a80d2b336-source.min[1].js	
SHA-512:	43264731C33800CAC5128369BE77C10B0658AF20705032B495FE3C2674C3BCF2A0E1970B4AA14191EB94EC8923709DAC3D7E83BB603A617AED3B9B8621EB03B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RC278c787435b94d148603e89a80d2b336-source.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RC278c787435b94d148603e89a80d2b336-source.js`..._satellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RC278c787435b94d148603e89a80d2b336-source.min.js', "null!==window.wdgtagging&&null!==window.wdgtagging.jsll&&function(t,n,i,s){n.loadJSLL=function(){var a,e,g={appId:\"surface\",version:\"4\",coreData:{env:t.getData(\"env\"),market:t.getData(\"langLoc\"),pageName:t.getData(\"gpn\"),pageType:t.getData(\"pageType\")}};(\"undefined\"!=typeof isUserSignedIn&&\"1\"===isUserSignedIn||s(\".msame_TxtTrunc.msame_Drop_active_name\").length)&&(g.isLoggedIn=!0),location.pathname.match(/\\/surface\\/business(|\\/.*)$/gi)&&(g.appId=\"surfaceforbusiness\"),g.prePageView=(a=t,e=i,function(){e.setMetaTag(\"awa-env\",a.getData(\"env\")),e.setMetaTag(\"awa-market\",a.getData(\"langLoc\")),e.setMetaTag(\"awa-pageName\",a.getData(\"gpn\")),e.setMetaTag(\"awa-pageType\

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RC4531a4e4108f48ab95bfce9b9140bf03-source.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	589
Entropy (8bit):	5.282207029013176
Encrypted:	false
SSDEEP:	12:jvgefCGWReDLLct/BefCGWReDLiLgU985SDqiKoufoAVNUwuGn/:DwSLct/BuwSpU985SZugM6wuGn/
MD5:	365CF77B4D31318EA79839B86F9A0769
SHA1:	41A3287A07D8DCFF9408094D3B2A9FE8F2C49C0B
SHA-256:	111505C49B833E6B23DB6632826EA4E1DBDC4387441320FE1796C9357C5931E4
SHA-512:	7B7ED4EF61DC3F74EC7D78E427120D1AABFD41FB51298BFEC49FEDD866FF3D67F1CA626E8B6C5DCBAF37B8F3FC2D9E352A4662B60EB7778AE8C5F8413E7FF6EB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RC4531a4e4108f48ab95bfce9b9140bf03-source.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RC4531a4e4108f48ab95bfce9b9140bf03-source.js`..._satellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RC4531a4e4108f48ab95bfce9b9140bf03-source.min.js', "null!=window.wdgtagging&&null!=window.wdgtagging.comscore&&function(g,n){var i=function(){n.init(\"//www.microsoft.com/library/svy/min/\")};g.category_all_status||g.category.analytics.status?i():g.category.analytics.queue.push(i)}(window.wdgtagging,window.wdgtagging.comscore,window.jQuery);");

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RC54b490a964b8430a93c0a4bea8ec38f8-source.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	19733
Entropy (8bit):	5.157454586914591
Encrypted:	false
SSDEEP:	192:2BcZj7BdmvowenfVbvnG/pyDzK3bzDRD4jxjT2HnCED5jwquHtq+1Ht8tR+OeBtU:20mvxB/hY1T2HnCW9duHw8HwYBiYhf7U
MD5:	05ACC84F97BE51402B9A4EE6FF30D840
SHA1:	1586B7CDD0FEABB53FFA8344C096F2D53A10BC11
SHA-256:	7A94A090954979C02CC00FC017C3B2F02BAFCE79F757F665AA2EE8C79B15276A
SHA-512:	E34948ECBC241BF9A141311509C3AC0FB6AE4E55813F6E8A4E552A940B51C2FFC311D957655B8CA3ECCA18AE56EFDA993E03C9D2696D6BAF6828194BE715590
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RC54b490a964b8430a93c0a4bea8ec38f8-source.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RC54b490a964b8430a93c0a4bea8ec38f8-source.js`..._satellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RC54b490a964b8430a93c0a4bea8ec38f8-source.min.js', "null!=window.wdgtagging&&null!=window.wdgtagging.jsll&&function(t,o,s){window.location.hostname;var i,r,n,c=window.location.pathname;o.tagMSStoreBehavior=function(){return\"PARTNERREFERRAL\"},o.isMicrosoftStore=function(t){return t.attr(\"href\").match(/microsoftstore/i)||t.attr(\"href\").match(/microsoft\\.com/i)&&(t.attr(\"href\").match(/\\/store/i)||t.attr(\"href\").match(/\\/p\\//i))},o.tagChooseContentType=function(t){return 0<t.find(\"img\").length||0<t.find(\"picture\").length?\"image\":e(t,\"class\",\"glyph-play\")&&(t.find(\"span\").length<=0||e(t.find(\"span\"),\"class\",\"screen-reader\"))?\"button\":e(t,\"class\",\"mscom-popup-close|m-back-to-top|video_pp_button|ps-lightbox-close\")?\

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RC5f812135e64f48ad85ea100034bc60a2-source.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	6332
Entropy (8bit):	5.333074281249945
Encrypted:	false
SSDEEP:	192:hBp3+u1vwkOIOU574BraYQNRmDzB3Jf1bjZ6x8br8bWHcGdXG84HQMqhuG:h3+hkOI5791UDzB3JhjZ6x8br8bWHcG9
MD5:	F64E679B1717879BC0780F2192800314
SHA1:	B98456A4CB3D3DE5C8F924BCF61D18FC9EDCED8F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RC5f812135e64f48ad85ea100034bc60a2-source.min[1].js	
SHA-256:	7F94B413F54CC56241EB8DE8212E72D7F9270B3DC462FA4DAA21EB58DFAECF73
SHA-512:	37A0EB9898FC632FF569EF7BEDFC9449ED692CEC56F421D7E6542AE9E5A51B0BFB8059D655F660BE34C13C683B7D1722013EB5DA6943510FC82111B699E530F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/2418adba327c/RC5f812135e64f48ad85ea100034bc60a2-source.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/2418adba327c/RC5f812135e64f48ad85ea100034bc60a2-source.js`..._satellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/2418adba327c/RC5f812135e64f48ad85ea100034bc60a2-source.min.js', "null!==window.wdgtagging&&null!==window.wdgtagging.jsll&&function(t,e,w,f){window.location.pathname;var m=window.location.href;w.wdgVideoTagging=!1,w.videoTaggingInit=function(){var g=awa.ct.captureContentPageAction;w.wdgAttachedEvent={},w.wdgVideoName={},awa.ct.captureContentPageAction=function(o){if(239<o.behavior&&o.behavior<253&&240!=o.behavior&&250!=o.behavior&&251!=o.behavior);else if(253==o.behavior)g(o);else if(240==o.behavior){var i=o.contentTags.vidid,d=o.contentTags.vidnm,c=!1,r=f(\".c-video-player > .f-core-player\").find(\"video\");r.length&&r.each(function(t){var e=this,a=f(e).closest(\".c-video-player\").attr(\"data-player-data\"),n=\"\";(a=JSON.parse(a)).metadata&&a.metadata.video

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RCa6da6c2ddf044453bdb4d0b0dafda95b-source.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	4711
Entropy (8bit):	5.322809763544589
Encrypted:	false
SSDEEP:	48:Dit/Bu/yvxiEgqDGYjE+zJ/Yilk8EE7meDj6+tiM70RN2vnVlapFWPb0QNhqRJnT:+BBhVnNQilOWmAeOxoFFHFNL2F+L2FC
MD5:	E19BFDDC7B50718B21FEF046E258F791
SHA1:	E9D78C4257C276D2FE9C4CC445AB593C647B17BE
SHA-256:	D5D03CAEE0D0AA5D97D708D5800EA791FC834F78C2456F3316216F93FC4F1C2F
SHA-512:	983101CC0FC1537D171AD5E1ED00557282A63C5383C068E41C67AFD79620DAA51DAA7F4A43615EF9EF51F13E2B3417238298C54B9114DA4434E920B74610FF0C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RCa6da6c2ddf044453bdb4d0b0dafda95b-source.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RCa6da6c2ddf044453bdb4d0b0dafda95b-source.js`..._satellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RCa6da6c2ddf044453bdb4d0b0dafda95b-source.min.js', "null!=window.wdgtagging&&null!=window.wdgtagging.jsll&&function(e,a,t){var i,s,r,c,n,d=location.pathname,o=\"MAIN\";d.match(/\\/surface\\/business\\/extended-service-warranty/i)?o=\"MAIN>DIV.cfb\":d.match(/\\/surface\\/devices\\/surface\\-pro\\/overview/i)?o=\"MAIN>DIV.surfacecom\":d.match(/\\/surface\\/devices\\/surface\\-pro\\/tech\\-specs/i)?o=\"MAIN>DIV.surfacecom\":d.match(/\\/surface\\/devices\\/surface\\-pro\\/for\\-business/i)?o=\"MAIN>DIV.pmp-devices\":d.match(/\\/surface\\/accessories\\/surface-dial/i)?o=\"MAIN>DIV#surface-accessories-dial\":d.match(/\\/surface\\/accessories\\/?/i)?o=\"MAIN>DIV#surfaceAllAccessories_Browse\":d.match(/\\/surface\\/devices\\/help\\-me\\-choose/i)?o=\"MAIN

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RCa7a16d61c0134716b6c5d59808f9fd26-source.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2964
Entropy (8bit):	5.2961274592152465
Encrypted:	false
SSDEEP:	48:DvTwxt/BuvTwcgU+XwgDz1bw6ajXXmvDTjurwRVG1zGJ:XwxBBGwLZvaXwHYK
MD5:	270B267DBA1C7BD9B95E23B5A4F1A9F7
SHA1:	64183812D38BC944360BD1F9F56AB9174666AF78
SHA-256:	D7D195354138AE8BE208C2B24AD3EAA3375FBC242964D348182AC2DC080D69E3
SHA-512:	9D41A48729E34EDE37B0B160634704CBA6809553B5A638075F5B9482A1F52A5355A322986BCD149D6243F8C8D427ECC2F2F15DC0307269DAF68E3F49D876C9BD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RCa7a16d61c0134716b6c5d59808f9fd26-source.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RCa7a16d61c0134716b6c5d59808f9fd26-source.js`..._satellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RCa7a16d61c0134716b6c5d59808f9fd26-source.min.js', "null!=window.wdgtagging&&null!=window.wdgtagging.jsll&&function(t,c,n){n(\".surface-clearfilters button\").on(\"mousedown\",function(){n(this).attr(\"data-bi-bhvr\",\"REMOVE\")}),n(\".c-checkbox input\").not(\".surface-hmc-ans-block INPUT\").each(function(){try{e=jQuery(this);var t=n(this).next(\"SPAN\").text();e.attr(\"data-bi-name\",c.tlcStr(t));var e=n(this),a=n(this).is(\":checked\")?\"APPLY\":\"REMOVE\";n(this).is(\":checkbox\")&&(a=n(this).is(\":checked\")?\"REMOVE\":\"APPLY\"),e.attr(\"data-bi-type\",\"option\"),n(this).attr(\"data-bi-bhvr\",a)}catch(i){c.debugLog(\"Error tagging name for Checkboxes section. Error: \"+i)}}),n(document).on(\"mouseenter\",\".c-choice-summary button\",functio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RCc0230152987c4e73b3230be623bd92e6-source.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	619
Entropy (8bit):	5.3119452210922375
Encrypted:	false
SSDEEP:	12:jvgefCGMBdct/BefCGMBILgU9GXuAwiKolzoAVvwuk32an/:Dizct/BuihU9GXuAjyMvwuGZn/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RCc0230152987c4e73b3230be623bd92e6-source.min[1].js	
MD5:	15A8E3B484FEB5A097F58EB54C823412
SHA1:	D380427635990EF65F2A280EFFE6EE067C5CB508
SHA-256:	4F04B818B5D8DB24C6C0D060B763FB82F3CBA84B4E681FCD22CB670146DA8235
SHA-512:	0E6A6EFCF0456AE6C354F07AFA2AF851BFFD0865F7ED5C9BB32C954F1B53DBDD3C7231B1D6FA795C491509F3578B775403F40F2D271BDB88A3B57512A952016
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RCc0230152987c4e73b3230be623bd92e6-source.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RCc0230152987c4e73b3230be623bd92e6-source.js`.._satellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RCc0230152987c4e73b3230be623bd92e6-source.min.js', "null!=window.wdgtagging&&null!=window.wdgtagging.clicktale&&function(g,a,i){var n=function(){i.init(\"755cc4ab-c4bf-46d8-a608-d3c5d66fabac.js\")};g.category_all_status||g.category.analytics.status?n():g.category.analytics.queue.push(n)}(window.wdgtagging,window.wdgtagging.util,window.wdgtagging.clicktale,window.jQuery);");

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RCce79330d434c45ca8ea9effba974a13d-source.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	5249
Entropy (8bit):	5.233880865452266
Encrypted:	false
SSDEEP:	96:oBBBaSi77a29c9pgO29Y8WNUQEimDaimItA:oBraSi77e69Y8W9mDDA
MD5:	9325ECB0077B332318FBE8045FC800FB
SHA1:	0EF3205368D41E0C9FE47FC67177A00025CD25B6
SHA-256:	51504116D4A1C1E09C96A1477B602AA7AE3859ABCC34DAC3DE9ED18AAFFA09A0
SHA-512:	72FBD280288BE81D155224809069507F5E8142844A9EBAF24D5EC07B5E3819CDA78466BD3442369DC7FF88319D8C2A2D36F6C16D0FDAB563886FF0E01CB63047
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RCce79330d434c45ca8ea9effba974a13d-source.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RCce79330d434c45ca8ea9effba974a13d-source.js`.._satellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/8feea6849a28/RCce79330d434c45ca8ea9effba974a13d-source.min.js', "null!=window.wdgtagging&&null!=window.wdgtagging.jsll&&function(c,g){c.lineage={main_sel:\"MAIN\",zone_id:\"a3\",sec_custom_sel:\"\",grp_custom_sel:\"\",pnl_custom_sel:\"\",subpnl_custom_sel:\"\",exclude_sec_sel:\"\"},g.getLineageName=function(e,a){return e.attr(\"data-lineage-name\")||e.attr(\"data-productid\")||e.attr(\"data-productid\")||e.attr(\"data-vg\")||e.attr(\"id\")||a},g.setLineageSection=function(e,a,t){var i=\"r\"+t+a;e.attr(\"data-bi-id\",i),e.attr(\"data-bi-name\")||e.attr(\"data-bi-name\",e.attr(\"data-productid\")||e.attr(\"data-productid\")||e.attr(\"data-vg\")||e.attr(\"id\"));var n=\"DIV[data-grid*=col-12],DIV[data-grid*=col-10],SECTION[data-grid*=col-12],SECTION[data-grid*=col-10],SECTION[data-bi-area=body]\"+c.lineage.grp_custom_

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RE1Mu3b[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 216 x 46, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4054
Entropy (8bit):	7.797012573497454
Encrypted:	false
SSDEEP:	48:zICvnyRHJ3BRZPcSPQ72N2xoiR4fTJX/rj4sFNMkk5/p1k2lPUmbm39o4aL7V9XH:10nvE724xoiRQJPrjpLKSFl9oX31Z1d
MD5:	9F14C20150A003D7CE4DE57C298F0FBA
SHA1:	DAA53CF17CC45878A1B153F3C3BF47DC9669D78F
SHA-256:	112FEC798B78AA02E102A724B5CB1990C0F909BC1D8B7B1FA256EAB41BBC0960
SHA-512:	D4F6E49C854E15FE48D6A1F1A03FDA93218AB8FCDB2C443668E7DF478830831ACC2B41DAEFC25ED38FCC8D96C4401377374FED35C36A5017A11E63C8DAE5C87
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE1Mu3b?ver=5c31
Preview:	.PNG.....IHDR.....J.....tEXtSoftware.Adobe ImageReadyq.e<...(iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c132 79.159284, 2016/04/19-13:13:40 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:A00BC639840A11E68CBEB97C2156C7FD" xmpMM:InstanceID="xmp.iid:A00BC638840A11E68CBEB97C2156C7FD" xmp:CreatorTool="Adobe Photoshop CC 2015.5 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:A2C931A470A111E6AEDFA14578553B7B" stRef:documentID="xmp.did:A2C931A570A111E6AEDFA14578553B7B"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.....DIDATx..\..UU.>.7..3....h.L..& j2...h.@.."........`U.....R"..Dq.&.BJR 1.4`$.200...I.....wg.y.[k/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RE42F9C[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 400 x 120, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	14105
Entropy (8bit):	7.973071221691316
Encrypted:	false
SSDEEP:	384:ZgAD2GO9YtbIGGE+5ghOadutFDfx9Fb5CEVzI3WW9+zPSUsL:ZF2V2t1z+sOQutFDfx9X0WIM67L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RE42F9C[1].png	
MD5:	77B18BAE1CB8B2CDE06B0833ED44B198
SHA1:	982AEB5057BA686BB47A3953A6CFA953DC88083B
SHA-256:	8A8D4DD97DC37736E0488DA65D317D2957745930D46A0611A9EECB3CBF52F85F
SHA-512:	40BD31E1B9566F227356E2CA56B10EF5821F0040A4D19F322ABF7B4375D53882AE1CD5C177770220BE7C21002ADA83BECE0A694A9CFE5CBBC34CAF032643600
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE42F9C?ver=135b
Preview:	.PNG.....IHDR.....x.....6.IDATx.....`...F..l.....p..8(<ffff.K..w.....It.S.....Z....&...d..5Ue...Uew...$9w.....~....a..... .Z...8.}.I...n.6./.lX.V.R.. .&..k..`..k..C.....1E#@...1..J.....]......W..$...3.$.....w.e.....V+@.p5.....y....^K..D.[&l.p..{>.....S.8..S.hP.S..... su/....._\.Z..W.....d.....5t..p..S<..S...-.....~..0.$..{.q.$.. .....y....N=.N\.t..!...@..R....3x.z.!,A.F.....vpp(.c..84....".....?.. .a...k.X@.....a.I2..9.#.W.\.?..../.H...5.`OP.qg.13..ui@.B.l.a.I...m....._.6..82....H.q...$C).7...g..W....@.w....s. 3.r..j.YB....!l.a..DA..A...AP....O.$#3l..\....P`(.pT...PU.o...3&w.H..+..xi...h....=.("..I.E..Y$l)...@...4..+....6.D].....y.o//._#D.....H...M.,a.....4~Y...@.V..@..6L.....`.F...D.`.u.jF%@K. M...!..\..../...sk....$IFD.."..V.@.-.P.n.....#*w...]}.....+...!,!&...I.....$.1.....q'..e..Y....a%..J...$..\r[..h7B.....JhFb.1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RE42Sb2[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 400 x 120, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	15153
Entropy (8bit):	7.968349888527871
Encrypted:	false
SSDEEP:	384:oB2l8krTpnbjlFRcbfGMAPbP2xY3+cauTjD:oB2fpnlHcSP2eaCX
MD5:	3BFDB27420A986F34F8BF60B81B4430B
SHA1:	8349CA28900A72C977DB2D1CAFC44DB57B231243
SHA-256:	6F7DB1165CCDCEA66E20D7BBF6F69BB88EEC525189FA470479A5B906B447D236
SHA-512:	FED1E339DFC7FD4C91B2C042DEA6117E10C5B5E7FA29E8C19AB60498CB7662924695B8BDAAE1CB53F3261134E4FBFAD094F79F42498D5D6EED911F1DA4AD5 5F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE42Sb2?ver=5d43
Preview:	.PNG.....IHDR.....x.....:.IDATx...E.C1.....CU...A..,i._.....G....L).9.....ZC.9.R..j..vc...G...}.s.w..q....jvv.Li....*.5=..Tfn..Sff..N.K.....C...G.....[..l}b.^i..>...J.` . .LI.hjl.(..Xq.]w..P.M.@L.6..M.F3m.43..e.c.,{...l[...?....?...:~<.s.mAp. .Rf.B..H.a..3`8.4.....B.@....!5%..ii.....p..4..~...G...;.E...h4...;".d.QG.r.B...h....mB@6+..g.xf<.....(... .>...a$...mM.fR..m....l..}~~;;...e.9s&.-[...{.X...o..<.....h.v....6w....u9.h,;1...@(.".p.".G...H...?.L.e.m!..3.;EZ..2).B....N..&E...k..`.<....`B .....E ...]..'.G.H8..r..~8.....2.D#...*.q h4....W.....~..K).....`...>.|._..._.\(.2....a...A....K.>Y.@.v*.l..@.i,.....C0.D.....c...;w.jjk.....~...b....?.....>}.....O..&.h).....!.'..@.....H.....C.PDAM....0.Y.]L.....$.o.a.9..."@.D.... [OKIE...x9.OP...PSS.....Nz..X..4..@....h..x|.....*223 -...4.[2Q',.&.v.i'7J!k.....4.o....._m....?!.f..m..j...?MQ..HD#HF0..X.n...,..N.:....K.....^...?..^...E.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RE4GG6p[1].htm	
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):	4901
Entropy (8bit):	5.197679477689848
Encrypted:	false
SSDEEP:	96:AxtrMzrHG3wQreAjreA/nreA3xreABfrxpjoLUJtMyUJt1dUJtzaU8cBCRp8cK4W:A+XrAeACAYAtrxeLSMyS1dSzanQCRmbD
MD5:	C2808C1FFF8BCA99C899DC970E72967B
SHA1:	BAE8B1BFDB18B50A4CE1508EC20ADC56D08909AF
SHA-256:	82D7AD5F3EE6E54DBCD0FDB04CC54BBAAA34B6BB3033B9819A867ABCD33E0D2A
SHA-512:	7E19F303DDDECFDD47145562B8A0009E1529D56A991FC7DD8609E73F58458E614C60502B506C16B491E14E8D2A5BA2DD1CB700FA7D0A1854CFA2466877BBB3(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod-video-cms-rt-microsoft-com.akamaized.net/vhs/api/videos/RE4GG6p
Preview:	{"captions":{"en-us":{"url":"https://prod-video-cms-rt-microsoft-com.akamaized.net/cms/api/am/videofiledata/RE4GG6p-enus?ver=f618","link":{"href":"/vhs/api/videos//captions/en-us","method":"GET","rel":"self"}}},"transcripts":{"en-us":{"url":"https://prod-video-cms-rt-microsoft-com.akamaized.net/cms/api/am/videofiledata/RE4GG6p-tscriptenus?ver=942b","link":{"href":"/vhs/api/videos//transcripts/en-us","method":"GET","rel":"self"}}},"snippet":{"activeStartDate":"2020-10-13T23:03:27","culture":"en-us","supplier":{"name":"","source":{"name":""}},"thumbnails":{"extrasmall":{"height":0,"width":0,"assetId":"RE4GScv","url":"http://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4GScv?ver=b6fa","link":{"href":"/vhs/api/videos//thumbnails/extrasmall","method":"GET","rel":"self"}},"small":{"height":0,"width":0,"assetId":"RE4GScv","url":"http://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4GScv?ver=b6fa","link":{"href":"/vhs/api/videos//thumbnails/sm

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RE4GScv[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop 21.2 (Macintosh), datetime=2020:10:09 21:46:49], baseline, precision 8, 1920x1080, frames 3
Category:	downloaded
Size (bytes):	1340772
Entropy (8bit):	7.965685949237803
Encrypted:	false
SSDEEP:	24576:QZ+8p58isujJJQxdnd9VhqfG/813+dDcHTr7xCNXFui2xbxRN7tLdM0dh0:QZ+gFwndhqfG/XcEui2xrpbM070

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RE4GScv[1].jpg	
MD5:	A5ADF472D2EA5E4060BC6D5C27E1E3C1
SHA1:	AD2AC6F3CB684A8B45801FD6B9E7232188AA1E1B
SHA-256:	7F33AA1BEBE733F2CED48C198C8CB8C6B6ACB17292C8324FAC469E35248AEF1C
SHA-512:	73A9449E0174399BF03E2D8D3C770946CA169C32A4A809EFE898295E79B5A53B7F2582B4D32402C23064F113C2E73F148E6D3041CEE16AF5E543FB51A81F0D9F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4GScv?ver=b6fa
Preview:	......Exif..MM.*.....b.....j.(.....1.....!...r.2.....i.....'.....'.Adobe Photoshop 21.2 (Macintosh).2020:10:09 21:46:49.....8.. .....".....*.(.....2.....H.....H.....Adobe_CM.....Adobe.d..... .....Z...."..... .....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWg w.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?.....#sH#....R.....G.W(.-.....u.b.f=7..... =.....k..G.r.@.L...G.cfg....V...W.c..3k..X.zwJ.....`...<...0..kK.$..-....[...?..]....#...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RE4GnH2[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 280 x 120, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	18006
Entropy (8bit):	7.980577669410109
Encrypted:	false
SSDEEP:	384:2IPAkntycWvk4VOF1Ci1LM/TsEjdkxg545f8jlpTnN3Vf:2YAktyZvkQOF1XqTsEjd4g5XrLPf
MD5:	19D16862BB146EEFD33E438DD16E31A3
SHA1:	B1A525805B621E8B447477CA4D7E67CC03620918
SHA-256:	18133B93233FBE33CF7C9D6333A66C7DC2603E9E6FEC7FA5DE83A61FC6A10592
SHA-512:	822CE799BD8F3599FA26C1CE02D9DB66809FAE07CC682051CF9FF48F4E2235A3EE1DC8D87C3EF1A9FEDF51D8FDD5D03A7FBF026A79C4231F10286A8E370EEA C0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4GnH2?ver=b98b
Preview:	.PNG.....IHDR.....x.....)..b..F.IDATx....}G.....u.".m.u..6b..j.V\#.m.....f.T.1....7.g..N2K..A..A..A.c...7..`.[n....>.l./..r.....H..y....X.....\4....*u..M-.&.725'.L.....d.3..4..5..8g.yO5 ....#.0K(..?M..Q:P8...itt..m....w..*...4.}..O....j..?.../.x.n.M..b.{.A.^r..{.o..).[.....#.?.x...9.....(@....V...q.....{.=..Yu.uYo.].A..LT.JnH....v^.5.0.C.....j...P9V..f.s..k.Q.....f.*~;../E..yV. g...PY..I..H....k.?.....&.....U...$..a..... D.5....#0+..f.....M&.._e~OM....K\..\|S. .....!..5k5A.)f.{..fl.b.v....A.i.~.....*.?E....9ff.U..#...|...|..X2..%c...w.Eu.....&.|.W...Ul.L./K. {C.....em...".v..i*...G-a...w.p.-h.'i..i.R.....W.....}3P..I..|....;V..WI&Y..^..P....J.*5..#....w<....q..*i.*.?..n....u.v...!T`a...:jU.*Bi...M..=...../....\mm5.,..B..J.X.`;.W.....%...Wt.y...q: <BWA....G....w.D.E.{.W..)..7.>.....h...".0..M.\z.w..}...Ix;.\.....Fg?...u...R...bJ.....h.....5.....1j.(..&....;@mX.F....%...=.X..W$..6(:.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RE4GyKc[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 400 x 120, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	18381
Entropy (8bit):	7.9792625595650435
Encrypted:	false
SSDEEP:	384:aCXj0xWxq4dpQax0gA6TnJcamFq1q5yNWiG2UB67NNA:ar2Uax0gxnNmF46yNi2UBwY
MD5:	05B38E0772D2F120BB5B9E38696B7D4D
SHA1:	547D26C57F77A703FF8426F5A6595756FD279417
SHA-256:	C6EB313F5573328DC784D5689298218E4D3C8352951DA8A7FBB9C4317F0B75A3
SHA-512:	F02C68D52A6015B48AD21BB1C68272D2717F20D5151A6B4BC290481C2C05275061D3F4D10ED1412A63DF885758E232E97B20F185D58C277A6EC5A11D7E8C0D9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4GyKc?ver=f8b8
Preview:	.PNG.....IHDR.....x.....G.IDATx...A.@@..0.B:....=D...Vbq.7.$.....jY.'u.7MU..{,..E..Y=....B33ff'ff.....2sh.....A.sM5z..g.d._...&.n..].....76....A`....@...\|D.v.Mb..)..cn.....3.. ..4V.g9.45$.9....h...}..\...1.H.O...w.-...'{.M..c;~....?.A.x.....W.C.....m_..W~..y.]w.....#...g|.].x.._0C...76.N.....g..[..7...x.S.....A.....g?.....g.Kp.;..<..lo.=...9]e.(..+..j...cTl ...R.YD.Ue..p...4..Y.r.....i...\.4A...[.)..w..:.cM.G.....g_.2....g.{..c.U:.=X|...f.Ngk....y....y-.{.S...D...LP.....|..'.).....*.6....jE.".M....C^G.7J68.v.N..3..Bd<..87p.{<..=.A.#..7.....,..V...9 w.....&.....Q..{..RK%...s..$HB.]..w..C.o.8\|.&...LR0.F.U..m.~..]..h4lm.f....>Z.....Y,.+....p9.....)dk..i...]....h{..0Neh.....$..Hc.K5li.&...i.1.Q.&;..`.....''H..U.-..D..&.H}...t .`.@..R-g.D...."..K....,*-.A+...A..p....)A.!.bP..rl6.....I.#.Hs:..A.2...#s...84 ..~H`.j.A;w:..F:..J..3.E.G...dT.w!..4..,P..5.#C..(g0..Xd{.{....w.Y.V.....1.04.(.B...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RE4eCGd[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 646 x 606, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	42774
Entropy (8bit):	7.8791899097860245
Encrypted:	false
SSDEEP:	768:sQ2CuP9zU1GqivmBHXAmAmL1G9niPaBN8Lrf0edsY8u5jdNJwZ3oGNIY3a7f01:sEuFU1GqSmfAmL1GY/HRdsY84jPE3oGP
MD5:	C3C53C5B75D39AD1509F63CC4498FA58
SHA1:	380A16E3364A7F6D04ADD23D49CFF963EA561DBF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RE4eCGd[1].png	
SHA-256:	72C1A1F399EB69E6700435F7376761AECD452499260D19E3D3C3FAFBB6FC47F7
SHA-512:	88D8FA1874CEC027F7989D94E1E1282FFA807023972EA104BE2CAEFAE8D5214973E63ED9E3E6CD0C479ADD95E4E6A8C5817EA093B118482E18FAFDCBE55A5C71
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4eCGd?ver=a2b1
Preview:	.PNG.....IHDR.....^.....)..;....sRGB.....gAMA.....a.....IDATx^....eWv.....U.WI2~....m...%(....i.`c[..`.....*.3.a@..z...A*.....2O.1J.p..}3%O.003%O..r.TU..G.=..{..9....72....^.....q.y..... .....`u|.0.ys....o..;...w..i.....[.....7...q.$}...,.....?v.v.....D...k..C..j....L..... .q.....#....W....0|.J..p..c.....}..8.g.7~.v.|..;5|..[....i.bU.....O}...../~....k....L.c.....7..M....a.....j.(5...s./-;KW...;..sn.?.k.z.._.e..<4\.....)`.....l..7.#3.E..1kM.....r...l./.=...../..y.Ol..3..-.E.....1..\.....o....r...nk..-.)...M.es..6..a^Zn./..ax..._!.....O.j".`.....Y...s_g...9./...j..Ic...V/....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RE4ehRf[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 646 x 606, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	10268
Entropy (8bit):	7.705440464889742
Encrypted:	false
SSDEEP:	192:PpMrugE/+88IBB5zpvqWICrXHd1nbAavMOw3t:2M+88gYanA8MOs
MD5:	D6F3749E348C369FA1BB840C1311759A
SHA1:	96C8CBB69CC329DDF91796579C9CBF4C11A25804
SHA-256:	5A81F94F15384B49AF177C759B3589AD926056DA18AFDFF554E95631E187D022
SHA-512:	3CDFD1C7838763E3AD6B389A327C0E36E6A4935C8824206F7117C308E157FC58B1C2D0396A438836079E89E3C5FBEA7BEC4F469CA5FC89E7CB2F8710AFC86BAD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4ehRf?ver=5ebb
Preview:	.PNG.....IHDR.....^.....)..;....sRGB.....gAMA.....a...'.IDATx^...o].y'...K.....q\.NZ....Mf.]....k..l%.[..w....{'..v2.....x1..#...#..A3.e.vlQ".}..C..H.?.s..|...=.&.E~...9..... .....T@(.....g.....Gb..t.I.=....>.br..5.~MCkay...$K..;/e_..M0....\|....#!....1..,..$.x!.}.....c....c.<L.A....{.N..(+....,.6F..b.sy..._...d?.:.U.....x5....N....j.W.F...C.\..`+I.u.`.....$^..."0(.!0X.*.I.....k.C...,_...kke)...e.zG0.....$/.K5.[..b..]..vn%6N.....^.....h|..c_U..\q....YR<.].&..."...Q.....-'.....N5.....P.!.{_...r....qY..f..*.....0...v...`.t.../.V..<..l$....V&I.. ..|.9I.?k/.9g.....'..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RE4hgqN[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 359x234, frames 3
Category:	downloaded
Size (bytes):	3464
Entropy (8bit):	6.8572628048727395
Encrypted:	false
SSDEEP:	48:BGKuERABs+ddddddddddddddddTFTvAzfJW0MdHW8Gu4Fjddddddddddddddd53m:BGdEVwFTvIR9sMsuBrLqJ9Y6r
MD5:	A33C257477A176B69241EC416CA74160
SHA1:	3DB79476AF74637111206FB26A77F3A1221D4E9D
SHA-256:	A3A8A262F6A5A57F517E7E362A45C727F61EFC6FC6B98DE3BA3BD29DBEBE65BD
SHA-512:	6918D084CED2141A4AABC52D4A1409F7AD563A8D98976E6E477706F2965D38BDD3EB0F48153BB3C7CB0EC5364B78FF40870FFCFC7561915182CDD5C00F2A4A7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4hgqN?ver=26d3.gif&q=60&m=6&h=235&w=375&b=%23FFFFFFFF&l=f&n=f&f=jpg&o=t&aim=true
Preview:	.....JFIF.....`.`.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....g..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...(...(...(...(...(...(...(...(....n.m....H...h.#..I....z.....o5..H....O.@..E..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..V.\|3.x...c."S...O...7..37.uQ.-..Xi.....5..}...e...+...*...>.....=-U..}.....d....-[L..N....5....o...M..m..m..%....^Qw.\^H^y]..ri6R..T.....xn....kn.P.5..ha.L\|.H....$n..5..._.cq..$.A.Ts2...Z...]

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RE4qZpg[1].wdp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG-XR
Category:	downloaded
Size (bytes):	18711
Entropy (8bit):	7.879125720338833
Encrypted:	false
SSDEEP:	384:e+KlooflhrVvMaESGZM0JXgOCrYX81Gx8I/x9AoQYJNZ:e+KoNhr61Sy348xn/36Af
MD5:	996AF36AF03A6BFB1654B69FC907A31B
SHA1:	1724A4F1DF9BFD5426111A0C2A7699EC52E549C6

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RE4qZpg[1].wdp	
SHA-256:	1CF63BEC6AC27FB198DEB2DB704602465A5AFCCED262F17C3F656D0FC1F0C37B
SHA-512:	8CE3C41F2FAFF99441A2374447B2091EB35E91239CB5D59C2D6EC1775037CC57BD0839FB5AD41FF32AFE11A3BBA3CEC9872765FCFCFCEFA0BFA62F719B5E851A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4qZpg?ver=06c1&q=90&m=6&h=180&w=321&b=%23FFFFFFFF&l=f&o=t&aim=true
Preview:	II.. ...$..o.N.K..=wv.....A.....$..B.....$..B.....H.....WMPHOTO..E.q.@..0...,8:B.. .....;..9h..... P.T....,0`.!...k.9"Jw.,)..iX`..0 .+..lru.2.k..1.9.. .0 nk....J.].6...6I...R.9^....W...S....x,..|..3..3.v.b..:.....K.4...,..M..:.-!..E.U.....u.Yk./N.(.....x.....Q...v.....!...2b7&"....(I>.w.[L.....%.I.6.....T&.....G...v.&...& .+aE.'...2.$'S..M.tn...u"!.f..e.^....8.(.\,H.....H)..q.O.I.M$k']:}.i..w$(.S..#J8.=%p#@vo/.. .P..c..$.8.Z....I^/....`H.E.....Pu..I..B.../.Uu.....&..!E..I*.(..E7...2*.../+@i!.G.'#.Q...?.&.}.H d...+.Z7...\.d..+&U|....v..R(u:...A!...ZI...,....Fg.!..M .|....#~..`.p...4F..MNF.R.....kB#-.d.$.I.2.....#..nc.@.....Y.4...`...Z.\@... @....q..B@...{..@^.rqQ.M...C.z.I}S..H..E..Gh...P2f..p<. 5H..g.Q.I.s`V5$I})...Fcc.K...*r....C.\.Pt.+.P.T.LC...H..A...5.w.!..4.....5.\..5.E!.B8.;.+h...B.P?....7...\.....~|..O).CtX.P.M.j..(..c1|.\....iX.....T.c..o.@..$f-.2.@.g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RE4r1Ep[1].wdp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG-XR
Category:	downloaded
Size (bytes):	18912
Entropy (8bit):	7.875288835593548
Encrypted:	false
SSDEEP:	384:DY2QLzc9RfVftc0CqhgfAOFcdAHGmGBJyJGDg/bygZ2e2dO3vf:02QcTcAyRFcdAmmQyJGDmyndS
MD5:	27D045ADF361EC7B7D5C536F3B8B2BCD
SHA1:	23FB7857805CC1901605B6F7E2FD49AC8FFFD015
SHA-256:	AD9834DD7E2580623DD3671171F7A9B8EA034BD3B0F201CBA586C251BB677337
SHA-512:	483EA397343993DCED1FCA62BBB8AABDA4CDA0E8880135FD6432C9D8BE6B2F1E0BCF3380AEC924A7B81809426C49CB3654CFDE0DD7D56CC4AA5E4A1B997DB5E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4r1Ep?ver=4ccc&q=90&m=6&h=180&w=321&b=%23FFFFFFFF&l=f&o=t&aim=true
Preview:	II.. ...$..o.N.K..=wv.....A.....$..B.....$..B.....ZI.....WMPHOTO..E.q.@..0..d..FHP.. .....<.....0.H.=o...v.V.n_h...n.O.j.9g.Z#. 2e..C.S.O.....%.0a..Yn..m....o=._.4q!2d.F...I.2P..f.~.D.....b(o].>..UF...4....} .n.p.\.;...G..z..).r.....@..^I.....I.>$N.T...G....P.i.1f....vs$.F..B....DL.Ho..P...5PL.GW.(...fk..... ,....x.tQ.)f.\z..L.....U.H....,+nE..d1Ot|....j.A.H%mQ..,....1Ku..7[br.IV..d..aD1.....d.^....F:d.J..8.3^B+.....,/..&.....D!....C(.Z....Zi....L.`.N...OVm>....88A2.}..T.^3..J..g...HJ.jQ. .dMW2.la.w..pJ.Gi.b:...,+2.Q.U..mSo.....f.....<Y.X....UKlL...Y.#..0<.W..!MN.....Z.L.\.zS...i.....d.5`..O.$25P..#u.C3.Vo*.#.c..>.|..K..D..@h....(.(.....(j-...BT.>rX.K.....B.-Th..i...n5..r..>l.:.S]K...k....I*f/.....R.M.NQ.<O.$. .....:.....h...o....d`.0.0@.r..8.p..L..8A...ii.2.....u..j.hV.f.(.U.....d...^.2....DoD.FLN..kJ.`..$.Sl.L..6....!..:.....>r..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RE4tWN0[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=12, height=730, bps=158, PhotometricIntepretation=RGB, orientation=upper-left, width=1300], baseline, precision 8, 1300x730, frames 3
Category:	downloaded
Size (bytes):	398309
Entropy (8bit):	7.892288915000026
Encrypted:	false
SSDEEP:	6144:7EFjUIpvcdPWMeHE+qFFLV0o1E14lGSxV+EmUmaFORjTocLceTzeuFEO0LxVH:7EXViMxZo1E14lGSmEmUmsmAocCDSH
MD5:	C8856BB199A5F55FDF8B988B3A25B507
SHA1:	46406EDB6248CE93F3771AF1D019C69F5E5BDEA3
SHA-256:	00ED24A1E4E60F4E4FA388035AAC5E8B07DCDB6A697754F39378D9BC9BB9818B
SHA-512:	31D603AAF02D67D5EA689E29F042A08DB811979BC1D2FF1B5469351E54B285314CC224DBA2DC5844CC176A1ACCFA22F36308DE4B6199DF98833378D2F76D424
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4tWN0?ver=466b
Preview:	......Exif..II*.....(.....1.....2.....i..... .....'.....'..Adobe Photoshop 21.1 (Windows).2020:04:09 20:11:04.....0231.....n.....v...(.....~.....1.....H.....H.....Adobe_CM.....Adobe.d..... .....Z....".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5 ....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw..... ...?....D..tN.ZRg..Nhp.=...o...r+...).5.....1.6\.....%.....Z.i.s.4t.g..O

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RE4yf9A[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 400 x 120, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	22420
Entropy (8bit):	7.980366544618822
Encrypted:	false
SSDEEP:	384:s+ZHeSW4mPxBdMafBW6EsCRIC6m1ApqzFvvLZo0UPbi2i1pB:NwX4m0UZpsSiLpB
MD5:	7770EA50C1F74B9C8B437DF7BAE41615

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RE4yf9A[1].png	
SHA1:	75E3C36CAA98358D0910D9DC99838C301F4F1C38
SHA-256:	C99E46243C0F2243437FC876B52528134276A79BB23F42F60E0A31D4638B46CB
SHA-512:	6939AE08FD68A5810F57D37A4AAA56639DEAA2DFBA02553DAD190542B112114A0763238E4420E91E52B25454BA9F61CBE4BA0B7B7CF7F4187252578DF8FCB7C C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4yf9A
Preview:	.PNG.....IHDR.....x..... .IDATx..y.d.U&.....R.U.U.U]..RkC.2...k..3...sl.....9.a..3....Y.....<....Hh.I-. ..u.....c.%..m>..~/.EVf....#.....+.~.....''..b.-..b.-..b.-..b.-..b.-..b.-..b.m.M..Q ....V.....S.\N~.....'.x...Jn(@ .1...^ .~.....C.c.|<..:.=.~.....}..L.....c.v..\..e...E.\...+PUup.~.@.4....k...."....iy.L....'}...o..!...@.u.\\.q.h{...v...KM.h..O.q.|5U....]........3...q.....<. .;..8}.u\..<.u]....^.gw{=.....v.v\.n.Z.k..].z..e~9.....iv..5../.S.....q0..._..b;..y...#....{.T...1^..&...[...y0t.....i;...q..q]......=.t..r..t=.....|.....9s.u-..l..l...c..&..n....w,.q..K..-....:....k28.....| L.....C...L.H.....{.._.....|..j..7-.v}.....[l'..e..G..Lomm=a..9jr.v.....*J-....n.w:.).s.^.I..g(.Rw]Ws.7..yr....0(0X..w-....K'N.#.*o...{r.>.A.#...._.p..#I..H...B0....b..et%..=d$.....}(#..d.....0 ?...w..k....;.@...r4..k.b...bYp~....f..../.O..._~...l".`.L.....t.YxGN.r...!...>B....G.4..|O. g.i..S*..7.J`...n38q~...C..^.~..,...9r..}.z

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ScriptResource[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	26954
Entropy (8bit):	4.516288580103467
Encrypted:	false
SSDEEP:	384:EMgviMjM4if38GmhXeC1QRwweTkBE9wbOY4Jf/JhRZ5h+73hNVt8oC4veONhLYVi:ZLEiJSdo11vIYHqb5Klo8v
MD5:	3DBD97A205B8CE59D755AB94F8C42964
SHA1:	B0520226342BBA131160A510BA3B57A1E8B7B80C
SHA-256:	36F7B9FE80A026A5D933855DE494AC6B7A4D01A93C26CE8A8737EED0C79367F4
SHA-512:	82BE6F1015CC346811EB736BD78F4949C855E49F8B4CC8493B22AE0F8D329EFA34205599E1138E57D33302B8A7B76F085DED053530B0F79D0DC71E257C99D80D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pembina.sharepoint.com/ScriptResource.axd?d=cIUfeLlIIpVJe0ra_eq80vJ2bC2Z2x5DSGiyl1HHlOpLsB3TbT7B_amVBaprUbr7J_tcdrfO71le-AtUnKFdU7zkoUcfSAypCyNz6IB3qClq6mHDKv8dxmiFOOgOH9LBJtHObekBtvUH3pz9lIvA5PJLgbeYcDB9so3475Nrsl41&t=58ba508e
Preview:	.var Page_ValidationVer = "125";..var Page_IsValid = true;..var Page_BlockSubmit = false;..var Page_InvalidControlToBeFocused = null;..var Page_TextTypes = /^(t ext|password|file|search|tel|url|email|number|range|color|datetime|date|month|week|time|datetime-local)$/i;..function ValidatorUpdateDisplay(val) {.. if (typeof(val.display) == "string") {.. if (val.display == "None") {.. return;.. }.. if (val.display == "Dynamic") {.. val.style.display = val.isvalid ? "none" : "inline";.. return;.. }.. }.. if ((navigator.userAgent.indexOf("Mac") > -1) &&.. (navigator.userAgent.indexOf("MSIE") > -1)) {.. val.style.display = "inline";.. }.. va l.style.visibility = val.isvalid ? "hidden" : "visible";..}..function ValidatorUpdateIsValid() {.. Page_IsValid = AllValidatorsValid(Page_Validators);..}..function AllValidators Valid(validators) {.. if ((typeof(validators) != "undefined") && (validators != null)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\SurfaceHome_Lg_LinkNav_Panel_2_image1[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1161
Entropy (8bit):	4.484268885657083
Encrypted:	false
SSDEEP:	24:twcB464wj4pR5N7GPzP+S2VlsRoOY4TLSzitiWjbr7Nzeh+8jw:VrALUzP+SygoCLSzipbr7vF
MD5:	6F974ACB4E979FD3445E79E49FE72B82
SHA1:	950ED5BC60777B284956E8CCC418346BB5F905E6
SHA-256:	85BFC00A602796E9A5D55DE82F47042EE0D8BD735B213D6AE5C6ECE995783458
SHA-512:	4DCCD2A891DBE8A923EDEA65FA43393881A19BDF294446C8B70BF7EDF5C5AE557A6D35C1CD5E704B8E531F9041354DE48567E638075A46D12BFEBFD95795DC 6A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/SurfaceHome_Lg_LinkNav_Panel_2_image1.svg?version=9257ec5f-8430-88a9-e2cd-c455f7ce172c
Preview:	<svg enable-background="new 0 0 27 21" viewBox="0 0 27 21" xmlns="http://www.w3.org/2000/svg"><switch><foreignObject height="1" requiredExtensions="http://ns.adobe.com/AdobeIllustrator/10.0/" width="1"/><path d="m26.325 15.745c.103.103.197.237.281.401s.155.338.211.52c.056.183.101.366.134.548s.049.345.049.486c0 .234-.049.459-.148.675-.098.216-.232.408-.401.577s-.361.302-.577.401c-.215.098-.44.147-.674.147h-23.4c-.234 0-.459-.049-.675-.148-.216-.098-.408-.232-.577-.401s-.302-.361-.401-.577-.147-.44-.147-.674c0-.141.016-.302.049-.485s.077-.366.134-.548c.056-.183.127-.356.211-.52s.178-.298.281-.401l2.925-2.926v-11.32h19.8v11.32zm-1.125 1.913c0-.038-.007-.091-.021-.162-.014-.07-.033-.141-.056-.211s-.047-.138-.07-.204-.049-.113-.077-.141l-2.856-2.84h-17.24l-2.855 2.841c-.028.028-.054.075-.077.141s-.047.134-.07.204-.042.141-.056.211c-.015.069-.022.123-.022.161l.042.042h23.316zm-19.8-5.358h9c0-.994.188-1.929.562-2.805s.888-1.641 1.54-2.292c.652-.652 1.416-1.165 2.292-1.54s1.812-.563 2.806-.563"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\SurfaceHome_Lg_LinkNav_Panel_2_image2[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	2700
Entropy (8bit):	4.0512327807053135
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\SurfaceHome_Lg_LinkNav_Panel_2_image2[1].svg	
SSDEEP:	48:Vrm52wylgV/NtnyzXzGb5ZGkOnYJR/Kn/ARttPMntx5fe5UP6:dr5o/XnyzXzGb5ZGkOnYJM/Ajt27B6
MD5:	AB93076893C8F78FCFF45E52EDEFF382
SHA1:	E7792E494227FB92724EF33EFAC24A102FB3F3BD
SHA-256:	B9AFCDFFE50AAE8D924F007A8CA6C2CF5F42C4B9C55FBA8AB274D26FD2CC7E0C
SHA-512:	93D5418572990F455297AA5CC27FDBDEFA544C4FD2882F4A772D513047ED229285071BBA39ABDC2CAD5D4625D0E89FC66AD72812B7534F9940659FB22177A375
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/SurfaceHome_Lg_LinkNav_Panel_2_image2.svg?version=da456df5-7733-1a20-6668-991b453cd479
Preview:	<svg enable-background="new 0 0 27 21" viewBox="0 0 27 21" xmlns="http://www.w3.org/2000/svg"><switch><foreignObject height="1" requiredExtensions="http://ns.adobe.com/AdobeIllustrator/10.0/" width="1"/><path d="m22.844 6c.3 0 .58.059.843.176.261.117.49.278.684.48.196.203.349.442.461.715.113.274.168.567.168.879v6.82c0 .969-.188 1.822-.568 2.561-.378.738-.878 1.358-1.505 1.857-.625.5-1.337.877-2.138 1.131-.802.254-1.625.381-2.47.381-.704 0-1.317-.043-1.838-.129-.519-.086-.982-.211-1.386-.375s-.768-.369-1.088-.615c-.323-.246-.645-.531-.966-.855-.323-.324-.658-.683-1.007-1.078-.347-.394-.745-.826-1.195-1.295-.241-.25-.484-.5-.731-.75s-.49-.504-.729-.762c-.525.25-1.045.5-1.562.75s-1.033.5-1.549.75l-1.292-2.918c-.494.516-.99 1.025-1.488 1.529s-.994 1.014-1.488 1.529v-16.652l10.062 10.5v-8.379c0-.312.057-.605.169-.879.112-.273.265-.511.459-.715.196-.203.423-.363.686-.48.263-.117.544-.176.843-.176.421 0 .766.075 1.039.223.274.149.49.344.651.586s.276.524.343.844c.067.321.11.653.129.996.018.344</svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\SurfaceHome_Lg_LinkNav_Panel_2_image4[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1230
Entropy (8bit):	4.465658582341525
Encrypted:	false
SSDEEP:	24:twcB464wjm3HwyrNSPXhypqHaG2Zzz7FfuKaEWbhyUAadSyh:VrCreXhygHaG29FfDS/fP
MD5:	9807E2D0143042B099454E83F29FD3C5
SHA1:	8FD51F53C496175F8C07733A8C17497E16B51F59
SHA-256:	B042FD8196D7BEB8048862F6E0819AE253980A415E123F88AC6816363DB3545A
SHA-512:	CEA0F87D718C623C0CA156BA311136932A6484F76A08698E87B9D89C13F5D05B45DB1E2B4E7ECB0D17C732F59B6C92C6A827B6058B51368D0ADFDC4F94AB2D2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/SurfaceHome_Lg_LinkNav_Panel_2_image4.svg?version=f06b4b40-4b8b-535a-1bdc-60d370824ced
Preview:	<svg enable-background="new 0 0 27 21" viewBox="0 0 27 21" xmlns="http://www.w3.org/2000/svg"><switch><foreignObject height="1" requiredExtensions="http://ns.adobe.com/AdobeIllustrator/10.0/" width="1"/><path d="m21.312 4.214c.716.312 1.363.711 1.94 1.196.579.484 1.071 1.034 1.478 1.646.407.614.72 1.276.94 1.989.22.714.33 1.455.33 2.224 0 1.066-.204 2.065-.61 2.999-.407.934-.965 1.749-1.672 2.446-.709.697-1.537 1.246-2.485 1.647s-1.963.601-3.045.601c-.846 0-1.671-.13-2.472-.391-.801-.26-1.54-.643-2.215-1.148l-3.126 3.077-9.375-9.231 10.938-10.769h9.375v3.714zm-10.937 14.111 9.375-9.231v-3.786c-.146-.032-.326-.054-.537-.066-.211-.013-.433-.024-.666-.037-.231-.011-.462-.03-.689-.054-.228-.024-.434-.066-.617-.126-.184-.061-.332-.143-.446-.247s-.171-.248-.171-.433c0-.209.077-.389.231-.541.155-.152.339-.228.55-.228.399 0 .792.004 1.178.012s.775.056 1.166.144v-1.694h-7.165l-9.376 9.231zm7.813-.902c.863 0 1.673-.162 2.429-.487.758-.324 1.418-.765 1.984-1.322s1.014-1.208 1.343-1.953c.33-.745.4</svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Surface_Home_Mosic_Fall_20_Duo_en-us_V2[1].png	
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, 1067x1204, frames 3
Category:	downloaded
Size (bytes):	110892
Entropy (8bit):	7.84635961999939
Encrypted:	false
SSDEEP:	1536:hzNYmYN5FcaiCGXWVepzrCmuMwtWQwLdilT56ALTkFlXPo7hHcJ9jgmmq:hzNYmYNHPiCiWkzrC+jL4lTw//wtlMq
MD5:	A6546766F19A898FE69B7AC27BFAA8AC
SHA1:	F5F98B45F64877D0FE91EB317AF9997364CCBE59
SHA-256:	A62911AEA3880C924C9530E34736DA99226B29088B5CA6F18219231751C38015
SHA-512:	979E594938743560CC48A6006C310F6C692DFE205CAA15E93E2F0450A5E4C9821021410A81F9354F206DC265CAF97FE4CE81D902FD2AA75BCE121EDB0CA336C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Surface_Home_Mosic_Fall_20_Duo_en-us_V2.png?version=54fef09d-3825-faa1-e9e1-5906428db7d4
Preview:	......JFIF.....+..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Surface_Home_Mosic_Fall_20_LaptopG_en-us_V2[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, 1067x1204, frames 3
Category:	downloaded
Size (bytes):	58433
Entropy (8bit):	7.6256639778743995
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Surface_Home_Mosic_Fall_20_LaptopG_en-us_V2[1].jpg	
SSDEEP:	768:14m3nvh0e/0vzGEmLnkvJxnB+5Pqqu+AvkwvdyMZpsx3WoudamFam2uU+:vaz5mLmBKCtdyMZpsx3G4m2uU+
MD5:	70C368372892A024EA4CE7B27E8F169A
SHA1:	D36BCE769DCEC2496426A28BB1634BB735E82A2F
SHA-256:	8792B1D4BECBB667179E4C55FA4B7F5CCC97E984B3B4AA7AE19FB44BC813EB5C
SHA-512:	F909B0497055C657F4523DBF0EE6F4EDF5B130F904B7A0FECCCF12588471B9B68F681BC7B84FBA5BB8849E5238AB8EE7A5DB2F291BFA471AE061C0F6E32EF7C7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Surface_Home_Mosic_Fall_20_LaptopG_en-us_V2.jpg?version=66aa72f1-33a1-112d-3853-bfa1abfe9767
Preview:	......JFIF.....+..... .....i./JV...&mh.....r.kZV..)JR.A3k^.2e.x.....V..+JR..)Lt.:S.:c...l..7C.....+Z..)J.)Lt.:c.:c....).....4..+JR..:S.)...Lt.....?k.....yiZ..)\t.)Lt.Jc.:c.<t.<t.:S..R.....iJ..)JR..Jc.Lt.Lt.<t.:R.....+JV..)JR..Jc.1..1..1..Jc.. .....+JV..)JS.)...Jc.:S.)...:S.....J..)JR..Jc.1...:R..JSc.k.....JV..)Jc.:R..Jc.1...JR.....F.R

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Surface_Home_Mosic_Fall_20_Studio_2_en-us_V2[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, 1067x1204, frames 3
Category:	downloaded
Size (bytes):	65223
Entropy (8bit):	7.654821000346925
Encrypted:	false
SSDEEP:	768:owa5TqsH9Rk5gw0PQE5pcx66V7sGFXsqR/Se/voVMQ7pryXHdo9MahGMn8jMHBa0:IzH9RkCKt9seSe/vKlgran8zIcijYeZ
MD5:	5B7962F8382200712B20A18026AB88D3
SHA1:	61D43D9EC3785CD4831CC44C3532E5F580B26195
SHA-256:	0E6E7B32EBBCFA08DD1E10F08B5CC5CAE44B5715FF6C088CB726F3B2E191AC91
SHA-512:	885D9AC6B62F9FE6E49B309F1D44E7BC3FC0FF05CBF7985452779EE7518223EABC41B9A606FEE72B94AB58CA69775D48CDDDAF5589FCCF7349A8C0B89E0D730C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Surface_Home_Mosic_Fall_20_Studio_2_en-us_V2.jpg?version=baee2e89-216e-2abc-0a9c-736048910609
Preview:	......JFIF.....+.....}$...I(..b.IP.....s.E;.....W.....X. .XX..h.@.),RYD...N@.....mw$.K.dR..,Y`....a}.....Y@...../.~.....8.._.>..,(..**Q(EK).)**.e.O....<.....).T...,BT.e.,YH.U.....*.E.P.Q,...)..T..}g.....p..F .x=..,...e.Yb...*X*..K*YS/.]k.. .....p?.>.x=.....YH...."......g.....8.._....R.%.*TT.Ie.....e.K.{..[.....p..>>.....@T...I`.....b.U...T.....{.HT....YR.R.B.`T...2...S.....c.....R*.... .P...).*..J.|R._..o....._.z0....%.....b.T..,P.).R.R._.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\amc.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	846707
Entropy (8bit):	5.1035574569321165
Encrypted:	false
SSDEEP:	6144:MEZACiZ9dyG1lBNZF6Z95+KpZ93+KmzvpRdU6mM+SMGquOa2+KT3zt/zXtRNtRQz:MEZxKiIscz+pjgn
MD5:	78BC6C5756DD54E705FCD94BBC264629
SHA1:	BD9E4652E0C43096B781927C67D97A54D3A2CD57
SHA-256:	77809B93020CFE3093F02B949773FD0ABF2F6F0E7ED3B6200B4D3CEE822EB05D
SHA-512:	928046D07405499DC3B4D2BE8E19D6454CE76868BF5AFD44B396E405BDD4A5A05D52C73A9ECDEDBDC2A38D912CE1855054A6E47B55C3FE013B209A355776D66
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://mwf-service.akamaized.net/mwf/css/bundle/1.57.8/west-european/default/amc.min.css
Preview:	@charset "UTF-8";./*! 1.57.8 | Copyright 2017 Microsoft Corporation | This software is based on or incorporates material from the files listed below (collectively, "Third Party Code"). Microsoft is not the original author of the Third Party Code. The original copyright notice and the license under which Microsoft received Third Party Code are set forth below together with the full text of such license. Such notices and license are provided solely for your information. Microsoft, not the third party, licenses this Third Party Code to you under the terms in which you received the Microsoft software or the services, unless Microsoft clearly states that such Microsoft terms do NOT apply for a particular Third Party Code. Unless applicable law gives you more rights, Microsoft reserves all other rights not expressly granted under such agreement(s), whether by implication, estoppel or otherwise.*/./*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */.html{font-family:sa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cartcount[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2566
Entropy (8bit):	4.393500974386876
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cartcount[1].htm	
SSDEEP:	24:KPv6HUY5+yAZFAXJqiXZXTMxPv6HUY5+yAZFAXJqiXZXTMK:EyHgyYFGMEZo9yHgyYFGMEZoK
MD5:	EB42BF181717EC1B1C4D9458A7AEA1C4
SHA1:	69FE74312A74D5D71FD4124F96D58D35AA1FFCFA
SHA-256:	8F6ABC9668C8AA27926673F6FD5118AFFCA717A124A565F96D4DE4143B96DFAB
SHA-512:	A73A12DCE699ED7E1F60EA6C6C097F68FB7397044A4E275C79A0206D3EA18986B606FD45E81E6704463827BC97A081352BEF59B79E3B5A024FD7C104F243C982
Malicious:	false
Reputation:	low
Preview:	.....<!DOCTYPE html>..<html>..<head>.. <title>title</title>..</head>..<body>.. <script>.. function getCartItemCountFromCookie() {.. var name = 'c artItemCount=';.. var allCookies = document.cookie.split(';');.. for (var i = 0; i < allCookies.length; i++) {.. var c = allCookies[i];.. while (c.charAt(0) === ' ') {.. c = c.substring(1);.. }.. if (c.indexOf(name) === 0) {.. return c.substring(name.length, c.length);.. }.. }.. return 0;.. }.... var count = getCartItemCountFromCookie();.... var parentHost = '';.. var parentOriginProtocol = '';.. var pare ntOrigin = '';.. try {.. parentHost = parent.location.hostname || '';.. parentOriginProtocol = parent.location.protocol;.. parentOrigin = parent.locat ion.origin;.. } catch {..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\experiments[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):	1080
Entropy (8bit):	4.929748278277592
Encrypted:	false
SSDEEP:	24:BkVz1Pvrd+DG5QBdNWokLh6gXklj7fdF7jm/3NU9XirdnKfYbT2xOQqLUHTe4YH9:Bwd+DG5QJGt6lStMdKfpFUUzrIKH46Pa
MD5:	AE85B50A45D1902D929AF8A2A6A235BE
SHA1:	5D40395C6574D1E8B5A90BD7C6FA0C3E005EA2F3
SHA-256:	8224B8B1C1E8ED9D781EC6F3099071E80B8CED4A09E010AF35E856E90705F022
SHA-512:	D6917976DBECAB0F50D1A02E94A6B2DE093B299FFA8C9FC4A2B59EA31CF9FCCBA7E7F8B6BDD5632DC20B3D546D03D4D61E6F00675C1C750D7F6AED532A725 CF7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://account.microsoft.com/bundles/scripts/experiments?v=dhMHbKozrGOgxx2MYXfMMYMDxUo0UcLjtgcfK8uL2iA1
Preview:	var MeePortal;(function(n){var t;(function(n){var t=function(){function n(){var t=this,n=this.getOptimizely();n||(window.optimizely=[],n=window.optimizely);n.push({type:" addListener",filter:{type:"lifecycle",name:"campaignDecided"},handler:function(n){return t.onActivated(n)}})}return n.prototype.onActivated=function(){window.portalExperi ments&&window.portalExperiments.setExperimentData()},n.prototype.getFrameworkName=function(){return"optimizely"},n.prototype.getExperimentData=function(){var r= this.getOptimizely(),n,t,i,u;if(!r||(n=r.get("state"),!n))return null;t=n.getExperimentStates({isActive:!0});i=[];for(u in t)i.push(u);return i.map(function(n){return t[n]}).filter (function(n){return!n.isInExperimentHoldback}).map(function(n){return{experimentId:n.id,experimentName:n.experimentName,variationId:n.variation.id,variationName :n.variation.name}})},n.prototype.getOptimizely=function(){return window.optimizely&&!!window.optimizely.get?window.optimizely:null},n}();n.OptimizelyExperiment

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\fbevents[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	91541
Entropy (8bit):	5.392815074748715
Encrypted:	false
SSDEEP:	1536:uM+OWt6w6aiSTxeosWXPwShThe7qv0a9sIOU1jaMu5Qm2B+SNSMngUSZYSlIUiGu:uOF+j5SVBYDGE
MD5:	9E0662842A501206D741C8B57826BCFA
SHA1:	3B6E7981C1DF69CD22FB0B43A765196BCDF465DF
SHA-256:	0E49C2B4E86D3FDA1DDA93EB1210A47712F7B091181B4E7C6DA2B3E6F8E86396
SHA-512:	B341E60A1D0ED8B654BACD3A99AF62EA535EB875EA12086E7F5F198E42D38D278B628E24BF87CC6283C10EBE7F2EDFA7A978A9EA4ED2C98C2B31276DA9A864 A0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://connect.facebook.net/en_US/fbevents.js
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\folder[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	276
Entropy (8bit):	6.585814504685036

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\folder[1].png	
Encrypted:	false
SSDEEP:	6:6v/lhPKM4nDspTnaQJb8jGWEUkPWHA3Vk8p:6v/7iMX9aQ/WEPP1lku
MD5:	18D9DBEB09F89965910D1613BFFB334A
SHA1:	97C76D2F8EE4A46583B5134BD69DFD4EF8300A35
SHA-256:	8DF012FF1F74AAFB752560FD2F5644701726E1581833134D7E728E9E06B55879
SHA-512:	C1A20AA0239F58F0BF38712276D2D489558C17967E413C26251FA239C3094D5362152EB49766C92C22D6847A3FAA2A109C2DE97CA996FBCD620D8C18F9F322AD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spoprod-a.akamaihd.net/files/fabric-cdn-prod_20201008.001/assets/item-types/32/folder.png
Preview:	.PNG.....IHDR... ... .szz.....tEXtSoftware.Adobe ImageReadyq.e<....IDATx.b`...`..F...N..@.H}..8.....`Bb.../...S#.X..).l.....w..}.Qs.!..`.b`..c`.....f .r..F8@..x...Q..9.u..... .l.4...R".?.Q..4.FC`.....#>.....x....VAv.Z[...?.._~_.m...Q.....P3.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\guestaccess[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	82140
Entropy (8bit):	5.575024714228852
Encrypted:	false
SSDEEP:	1536:Plggu7WXBOxSPSW8N6fGNNKQuynfeTJs2wVXluy0H3c:PLuCCGeTKQuAfpVXluy
MD5:	6EAD9DE805A8D89ACC7F98AF81338D19
SHA1:	9C8F803BC2B43F12446A92D79FEB38886F48DDE6
SHA-256:	D1150084819A67EE32142D7CC8E18672186A521C5623DC63A91DC82667AEBE8D
SHA-512:	04A71F5FDEA248FE703C10FDE02502FB1C37CAB7CA66CFFD3AA4DBB5D45C1329B274BB680B8A1D2D2D05D5F823015066A402B4AEC92A107E2C34D85B0072B262
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\guestaccess[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://pembina.sharepoint.com/teams/BOandP/_layouts/15/guestaccess.aspx?share=Ev8UHcgPkQRPnPpDIa8PTeUBDnUZj2epg0IcLzD6O0XQNQ&e=5:GyiSQ3&at=9
Preview:	..<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">..<html xmlns:o="urn:schemas-microsoft-com:office:office" lang="en-us" dir="ltr">..<head><meta name="GENERATOR" content="Microsoft SharePoint" /><meta http-equiv="Content-Type" content="text/html; charset=utf-8" /><meta http-equiv="Expires" content="0" /><meta name="Robots" content="NOHTMLINDEX" /><meta charset="UTF-8" /><meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1" /><meta http-equiv="X-UA-Compatible" content="IE=edge" /><link id="favicon" rel="shortcut icon" href="/_layouts/15/images/favicon.ico?rev=47" type="image/vnd.microsoft.icon" /><title>...Sharing Link Validation..</title>...<style type="text/css" media="screen, print, projection">.. ..html{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}figcaption,figure,ma

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC134
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/info_48.png
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po..... .....X..;.=.P...../...+...9./..s.....9..|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0..''/n/.c...&.{.ht..?....A..I{.n.....|....t.....N}..%.v...:.E..i....`....a.k.mg.LX..fcFU.fO-..YEfd.}...~.''.. ....}l$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a... .N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a)..t..e.j.W.....C<.1.....c..l1w....]3%....tR;,..3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\insight.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	965

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\insight.min[1].js	
Entropy (8bit):	5.054069298581068
Encrypted:	false
SSDEEP:	24:cwpn36OZd9+zHGUGskGPGCGbYMidGwidGifidGslidGkidGkidGVyy33UjUUuH7a:936V/zk8jA/S5SPSzlSNSDSuyy33UjUC
MD5:	1682C15C32A384857CF7BB18701FD5CF
SHA1:	BD8F13BC5354C361FECF6B487F8A5DD68F3BBDAB
SHA-256:	F10B9B0C4107CA5A40A5C69B1AC91A8948D84F39893DEE6B429CDBDB05887093
SHA-512:	33ADA4C71B7016A08F82F77BF8084F038A689B8F4BBD53F197F14FE7D8B8E6B73306AE0029FB802395B18FE7AF48FC13DC9C528D07635D3D7639ECA2750B66B7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://snap.licdn.com/li.lms-analytics/insight.min.js
Preview:	!function(){"use strict";function s(n){return/^\d+$/.test(n)}var n=function(n,t){for(var a=0,i=n;a<i.length;a++){var r=i[a];if(parseInt(r,10)%100<t)return!0}return!1}(function(n){var t={},a=[];if(n._bizo_data_partner_id&&(t[n._bizo_data_partner_id]=!0,a.push(n._bizo_data_partner_id)),n._bizo_data_partner_ids)for(var i=0,r=n._bizo_data_partner_ids;i<r.length;i++){!t[d=r[i]]&&s(d)&&(t[d]=!0,a.push(d))}if(n._linkedin_data_partner_id&&!t[n._linkedin_data_partner_id]&&(t[n._linkedin_data_partner_id]=!0,a.push(n._linkedin_data_partner_id)),n._linkedin_data_partner_ids)for(var e=0,_=n._linkedin_data_partner_ids;e<_.length;e++){var d;!t[d=_[e]]&&s(d)&&(t[d]=!0,a.push(d))}return a}(window),75)?"https://snap.licdn.com/li.lms-analytics/insight.beta.min.js":"https://snap.licdn.com/li.lms-analytics/insight.old.min.js",t=document.createElement("script"),a=document.getElementsByTagName("script")[0];t.async=!0,t.src=n,a.parentNode&&a.parentNode.insertBefore(t,a)}();.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jquery-3.3.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	86929
Entropy (8bit):	5.289492706499139
Encrypted:	false
SSDEEP:	1536:aLiBdiaWLOczCmZx6+VWuGzQNOzdn6x2RZd9SEnk9HB96c9Yo/NWLbVj3kC6ta:+kn6x2xe9NK6nC6E
MD5:	378087A64E1394FC51F300BB9C11878C
SHA1:	0C3192B500A4FD550E483CF77A49806A5872185B
SHA-256:	4FE68FA216176E6D1F4580E924BAFECC9F519984ECC06B1A840A08B0D88C95DE
SHA-512:	9A2C70516EA0C8C37C7F072F214DE0AFD5DDEB643C6B5D3FA8ADE3EF8D2CE40BDF8B1B1194BAD296E9075562701EE7DAE48B18144B1CD2D735328BE5A3AC0BE6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/_h/46c44584/coreui.statics/externalscripts/jquery/jquery-3.3.1.min.js
Preview:	/*! jQuery v3.3.1 | (c) JS Foundation and other contributors | jquery.org/license */..!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery requires a window with a document");return t(e)}:t(e)}("undefined"!=typeof window?window:this,function(e,t){"use strict";var n=[],r=e.document,i=Object.getPrototypeOf,o=n.slice,a=n.concat,s=n.push,u=n.indexOf,l={},c=l.toString,f=l.hasOwnProperty,p=f.toString,d=p.call(Object),h={},g=function e(t){return"function"==typeof t&&"number"!=typeof t.nodeType},y=function e(t){return null!=t&&t===t.window},v={type:!0,src:!0,noModule:!0};function m(e,t,n){var i,o=(t=t||r).createElement("script");if(o.text=e,n)for(i in v)n[i]&&(o[i]=n[i]);t.head.appendChild(o).parentNode.removeChild(o)}function x(e){return null==e?e+"":"object"==typeof e||"function"==typeof e?l[c.call(e)]||"object":typeof e}var b="3.3.1",w=function(e,t){return new w.fn.init(e,t)}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jquery-ui.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	238314
Entropy (8bit):	5.145714836445267
Encrypted:	false
SSDEEP:	3072:2xDk6UPS1lippePllYI7pSDzOyAskRsPoeQ9+SuC:yU+lgtYIUGeQ9XuC
MD5:	DFE3ECF96456F8CAFC12A7F48DE6B8C8
SHA1:	9927AFBB31DF93A76977A676A933B7E3696D61BA
SHA-256:	E09639315704980552B92EAAE21F66AF00A6E8A371F757F76B0B12420C2ED2A7
SHA-512:	3D892EE75916931C6E8743A24078BC20DC1F0C455C11EF49601899080DB51B421319D11453BB1C1214F2BADB7AF632B9F75BCA2660613CC3FEC9831DE89F3C9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ajax.aspnetcdn.com/ajax/jquery.ui/1.11.1/jquery-ui.min.js
Preview:	/*! jQuery UI - v1.11.1 - 2014-08-13.* http://jqueryui.com.* Includes: core.js, widget.js, mouse.js, position.js, accordion.js, autocomplete.js, button.js, datepicker.js, dialog.js, draggable.js, droppable.js, effect.js, effect-blind.js, effect-bounce.js, effect-clip.js, effect-drop.js, effect-explode.js, effect-fade.js, effect-fold.js, effect-highlight.js, effect-puff.js, effect-pulsate.js, effect-scale.js, effect-shake.js, effect-size.js, effect-slide.js, effect-transfer.js, menu.js, progressbar.js, resizable.js, selectable.js, selectmenu.js, slider.js, sortable.js, spinner.js, tabs.js, tooltip.js.* Copyright 2014 jQuery Foundation and other contributors; Licensed MIT */..(function(e){"function"==typeof define&&define.amd?define(["jquery"],e):e(jQuery)})(function(e){function t(t,s){var n,a,o,r=t.nodeName.toLowerCase();return"area"===r?(n=t.parentNode,a=n.name,t.href&&a&&"map"===n.nodeName.toLowerCase()?(o=e("img[usemap='#"+a+"']")[0],!!o&&i(o)):!1):(/input|select|textarea|button|obje

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\launch-EN7506e353034849faa4a18bc4c20e727c.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	143426

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\launch-EN7506e353034849faa4a18bc4c20e727c.min[1].js	
Entropy (8bit):	5.1526712975756475
Encrypted:	false
SSDEEP:	3072:XuosYOHsup2LWDC5NMECzwjUW+6r1GPG4xArt8SuELAN:XxsEuiWDC5NfCzl6r1GPG4xy8Sa
MD5:	5BE22C3A8F01475859B30FE615B65400
SHA1:	E04ED1B47626AB6F77FCFF284E77D3491267F172
SHA-256:	1E805A1AF02B458DEB1FF89F5060054CE3935310A82F3AC6E85FC37B529BA112
SHA-512:	14F752F96331BFF1F84672DEEC384D7A36AB2975EE72B81F2AD03BE9A5E6B9E0DA002A8A1DC086916438B82D1108B8A4E00AC9F76FCFC23F68330B201B457C6D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/launch-EN7506e353034849faa4a18bc4c20e727c.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/launch-EN7506e353034849faa4a18bc4c20e727c.js`..window._satellite=window._satellite||{},window._satellite.container={buildInfo:{minified:!0,buildDate:"2020-11-17T00:12:40Z",environment:"production",turbineBuildDate:"2020-08-10T20:14:17Z",turbineVersion:"27.0.0"},dataElements:{"JSLL RedTiger":{defaultValue:"",modulePath:"core/src/lib/dataElements/customCode.js",settings:{source:function(){return 0<$("#primaryArea[data-m]").length&&awa.isInitialized}}},MSCC_Consent:{defaultValue:"",modulePath:"core/src/lib/dataElements/customCode.js",settings:{source:function(){return!("undefined"!=typeof window.mscc&&"function"==typeof window.mscc.hasConsent&&!window.mscc.hasConsent())}}},"Surface - All Pages":{defaultValue:"",modulePath:"core/src/lib/dataElements/customCode.js",settings:{source:function(){return!(!location.pathname.match(/\/..\-..\/surface\/?/gi)||location.pathname.match(/\/..\-..\/surface\/business\/?/gi))}}}},"Surface - EN-US

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\meBoot.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	151027
Entropy (8bit):	5.552274047196116
Encrypted:	false
SSDEEP:	3072:SaTI1rl1+zRzNKTA3D9BonfZliweLS1SP:lcVI1obiFLS1SP
MD5:	6BA6782F526D5E602B5F9318E6A18CBD
SHA1:	9A103DB16D3FD5E6B350391FE7586F0D21AFAFB1
SHA-256:	8E15F620D6B1B87150ADDEA534DE7C1BE6D7A48F2DB64B47FE8A7B02FAD8F608
SHA-512:	A03A97A68057EB2F151441E6B04AFF98A9F919A941FDCF7338476BAE61443A22036163EB4ABA1F6C695DEB4DBB63B8C7DE981EE6F1CD1418F5EB1F439AF76067
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://mem.gfx.ms/scripts/me/MeControl/10.20300.4/de-DE/meBoot.min.js
Preview:	MeControlDefine("meBoot",["exports","@mecontrol/web-inline"],function(t,A){"use strict";var s=function(){},i={},u=[],p=[];function w(t,e){var n,r,o,i,a=p;for(i=arguments.length;2<i--;)u.push(arguments[i]);for(e&&null!=e.children&&(u.length||u.push(e.children),delete e.children);u.length;)if((r=u.pop())&&void 0!==r.pop)for(i=r.length;i--;)u.push(r[i]);else"boolean"==typeof r&&(r=null),(o="function"!=typeof t)&&(null==r?r="":"number"==typeof r?r=String(r):"string"!=typeof r&&(o=!1)),o&&n?a[a.length-1]+=r:a===p?a=[r]:a.push(r),n=o;var c=new s;return c.nodeName=t,c.children=a,c.attributes=null==e?void 0:e,c.key=null==e?void 0:e.key,c}function b(t,e){for(var n in e)t[n]=e[n];return t}function d(t,e){t&&("function"==typeof t?t(e):t.current=e)}var e="function"==typeof Promise?Promise.resolve().then.bind(Promise.resolve()):setTimeout;var l=/acit|ex(?:s|g|n|p|$)|rph|ows|mnc|ntw|ine[ch]|zoo|^ord/i,n=[];function a(t){!t._dirty&&(t._dirty=!0)&&1==n.push(t)&&e(r)}function r(){for(var t;t=n.pop();)t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\me[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	30819
Entropy (8bit):	5.438420140342225
Encrypted:	false
SSDEEP:	384:iN7XrUJds35bd8cAjYjN7XrUJds35bd8cAjYBN7XrUJds35bd8cAjYu:4w25Ldw25L3w25Lu
MD5:	EED30CF98CDE4FB4E32D10130858B3EC
SHA1:	2276B2742143A088868D9DDA30AE0117CA90EB66
SHA-256:	B8A8938715325C226A67ED0AD6251FE46425482A0997B7810B618C102A125833
SHA-512:	0C1FD94C7D9BD23B7DD5AE30023D6AA79F997D092C5B720350ABA5E10ABC2243BBA70B53F37769599A6D6456FDF349A2357FF6FD19D6226A812A706A2F45059
Malicious:	false
Reputation:	low
Preview:	Copyright (C) Microsoft Corporation. All rights reserved. --><!DOCTYPE html> ServerInfo: BY1PPF30EE91173 2020.10.23.21.27.05 Live1 Unknown LocVer:0 --> PreprocessInfo: azbldrun:AzBuildW2-Ha13, 2020-11-23T03:56:21.9041428-08:00 - Version: 16,0,28799,16 --> RequestLCID: 1033, Market:EN-US, PrefCountry: US, LangLCID: 1033, LangISO: EN --><html dir="ltr" lang="EN-US"><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"/><base href="https://login.live.com/pp1600/"/><noscript><meta http-equiv="Refresh" content="0; URL=https://login.live.com/jsDisabled.srf?mkt=EN-US&lc=1033&uaid=6e9e863e44bb415451f409f802860ffc"/>Microsoft account requires JavaScript to sign in. This web browser either does not support JavaScript, or scripts are being blocked. To find out whether your browser supports JavaScript, or to allow scripts, see the browser's online help.</noscript><title>Windows Live ID</title><meta name="robots" content="none" /><meta name="PageID" co

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\meversion[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\meversion[1].js	
Size (bytes):	27565
Entropy (8bit):	5.2402301560612985
Encrypted:	false
SSDEEP:	768:MdY26BzK4ey2FvZ60dQCn16JD2BlRnusqer6tAH6teJuN:B2AzK4ey2FvZRdQ3JD2BXAY6tAH6teJc
MD5:	9A79A9DEB44AD1E118A5F26E2709E2FD
SHA1:	2637540F65B175FE8D18CA564BBA2A1F7C223364
SHA-256:	6FFF602306E9607C1A29F5E8FC076C8FC93B3BCB131F6809C1409F3D9CA5642A
SHA-512:	E6622A15D490E44D959F413052D340039FCD989E6847DC831A6AD402B0FD7932270DE25E965CAC607A5CAC333ED3633EC881E3B774CBE4047863C6939407AA5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://mem.gfx.ms/meversion?partner=OfficeProducts&market=de-ch&uhf=1
Preview:	window.MSA=window.MSA||{};window.MSA.MeControl=window.MSA.MeControl||{};window.MSA.MeControl.Config={"ver":"10.20300.4","mkt":"de-DE","ptn":"officeproducts","gfx":"https://mem.gfx.ms","dbg":false,"aad":true,"int":false,"pxy":false,"msTxt":false,"rwd":true,"telEvs":"PageAction, PageView, ContentUpdate, OutgoingRequest, ClientError, PartnerApiCall, TrackedScenario","remAcc":true,"main":"meBoot","wrapperId":"uhf","cdnRegex":"^(?:https?:\\/\\/)?(mem\\.gfx\\.ms(?!\\.)|controls\\.account.microsoft(?:-int|-dev)?(\\.com)?(:[0-9]{1,6})|amcdn\\.ms(?:ft)?auth\\.net(?!\\.))","timeoutMs":30000,"graph":false,"aadUrl":"https://myaccount.microsoft.com","msaUrl":"https://account.microsoft.com/"};window.MeControl=window.MeControl||{};window.MeControl.Config={"ver":"10.20300.4","mkt":"de-DE","ptn":"officeproducts","gfx":"https://mem.gfx.ms","dbg":false,"aad":true,"int":false,"pxy":false,"msTxt":false,"rwd":true,"telEvs":"PageAction, PageView, ContentUpdate, OutgoingRequest, ClientError, PartnerApiCall,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\microsoft-365[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	168870
Entropy (8bit):	5.329993190167727
Encrypted:	false
SSDEEP:	1536:GkqHmIRldF8J9Zm4nzKF5ZHiKh1LGYhz3jEj9TNfHx7EmI9o/RLRPMUiUdyLPjiN:GhlRld4LUSY0RLRPMUixjo
MD5:	54650772932C3AA703551AD694B67A58
SHA1:	BE4C7D271D8A369C03D43F3EAF12F9D1968AC908
SHA-256:	F6FA288F9211FB47D887C3B47DE01FA326E5B57F97223F407CE2DB9F85A0DC39
SHA-512:	821490C9206C2555B55874CB832A7336D34DB7C41BF3467232DD3BA445749ED261BD81CE612F964E169BA80F9A40D0B86E27B4B004A9599C490D8F053E1C8990
Malicious:	false
Reputation:	low
Preview:	......<!DOCTYPE html>..<html lang="de-ch" dir="ltr">..<head data-info="{"v":"1.0.7621.39544","a":"79bd7e7a-c7af-489d-98c8-deee844d15c4","cn":"OneDeployContainer","az":"{did:92e7dc58ca2143cfb2c818b047cc5cd1, rid: OneDeployContainer, sn: marketingsites-prod-odnortheurope, dt: 2018-05-03T20:14:23.4188992Z, bt: 2020-11-13T05:58:08.0000000Z}","ddpi":"1","dpio":"","dpi":"1","dg":"uplevel.web.pc.ie","th":"default","m":"de-ch","l":"de-ch","mu":"de-ch","rp":"/de-ch/microsoft-365","f":null,"bh":{}}">.. <meta charset="UTF-8" />.... <meta http-equiv="x-ua-compatible" content="ie=edge" />.. <meta name="viewport" content="width=device-width, initial-scale=1" />.. <title>Microsoft 365 jetzt mit Office&#16

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\mwf-video-player-main.var.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	237078
Entropy (8bit):	5.3870591154530905
Encrypted:	false
SSDEEP:	3072:oa+l6JHGf0K21/HxmsYVy8Hrqcp5pbwk/F7LLIm0QYE5cOjJ:j+oJQI1QsqPqsfbvdhcy
MD5:	B004CE88CFD385695461C69476147B0F
SHA1:	49A83FF06933C77AA3AD6B1D37672911A1B1C78F
SHA-256:	AEFFEB518D9839CB9C071119A86619A218DAA1CBBD6BA75F204C53EAA8E0B4FE
SHA-512:	1EA0A3A4EF350D2DF0B1AFE88AAFA99D0EF7020AA559462A67DE5D8C0B056CB7040D64FAE534A3950C5CDF70B92317AB44A37ABA3C27B185127A7A9A359BFAF2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.onestore.ms/cdnfiles/external/mwf/long/v1/v1.23.1/scripts/mwf-video-player-main.var.min.js
Preview:	var clienttelemetry_build;!function(t){t.version="2.4.0"}(clienttelemetry_build||(clienttelemetry_build={}));var Microsoft;!function(t){!function(t){!function(t){t[t.BT_STOP=0]="BT_STOP",t[t.BT_STOP_BASE=1]="BT_STOP_BASE",t[t.BT_BOOL=2]="BT_BOOL",t[t.BT_UINT8=3]="BT_UINT8",t[t.BT_UINT16=4]="BT_UINT16",t[t.BT_UINT32=5]="BT_UINT32",t[t.BT_UINT64=6]="BT_UINT64",t[t.BT_FLOAT=7]="BT_FLOAT",t[t.BT_DOUBLE=8]="BT_DOUBLE",t[t.BT_STRING=9]="BT_STRING",t[t.BT_STRUCT=10]="BT_STRUCT",t[t.BT_LIST=11]="BT_LIST",t[t.BT_SET=12]="BT_SET",t[t.BT_MAP=13]="BT_MAP",t[t.BT_INT8=14]="BT_INT8",t[t.BT_INT16=15]="BT_INT16",t[t.BT_INT32=16]="BT_INT32",t[t.BT_INT64=17]="BT_INT64",t[t.BT_WSTRING=18]="BT_WSTRING",t[t.BT_UNAVAILABLE=127]="BT_UNAVAILABLE"}(t.BondDataType||(t.BondDataType={}));t.BondDataType;!function(t){t[t.MARSHALED_PROTOCOL=0]="MARSHALED_PROTOCOL",t[t.MAFIA_PROTOCOL=17997]="MAFIA_PROTOCOL",t[t.COMPACT_PROTOCOL=16963]="COMPACT_PROTOCOL",t[t.JSON_PROTOCOL=21322]="JSON_PROTOCOL",t[t.PRETTY_JSON_PROTOCO

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\mwf-west-european-default.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\mwf-west-european-default.min[1].css	
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	556551
Entropy (8bit):	5.221740865051638
Encrypted:	false
SSDEEP:	6144:rkR57iqbPXIB5UR5vWenR5xWeMFdBjL+ks0EcU0MWEsuWe5fXbHfxlN/FNCn/Lpt:PYz0GKYcw
MD5:	5582719A793D8D70C369645A28698466
SHA1:	F4B2D75F1E55D65CF87DFB3E2A856A7C2D917A45
SHA-256:	301A9A7613FB8A2F5D5A12D5B23949E2B52849402A87FFE4D33DFBD7774C61ED
SHA-512:	AF00AC2F81D371BEC64E580005AB0BF57A0AA5F21E534BBC47A837069CB22B66A43A677F0B0188AB1946AF0AB6BDF4B4176329D40B35545E91D65C9E23F29FEB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.onestore.ms/cdnfiles/external/mwf/long/v1/v1.23.1/css/mwf-west-european-default.min.css
Preview:	@charset "UTF-8";/*! @ms-mwf/mwf - v1.23.1+5118857 | Copyright 2017 Microsoft Corporation | This software is based on or incorporates material from the files listed below (collectively, "Third Party Code"). Microsoft is not the original author of the Third Party Code. The original copyright notice and the license under which Microsoft received Third Party Code are set forth below together with the full text of such license. Such notices and license are provided solely for your information. Microsoft, not the third party, licenses this Third Party Code to you under the terms in which you received the Microsoft software or the services, unless Microsoft clearly states that such Microsoft terms do NOT apply for a particular Third Party Code. Unless applicable law gives you more rights, Microsoft reserves all other rights not expressly granted under such agreement(s), whether by implication, estoppel or otherwise.*//*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css *

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\print-icon[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	173
Entropy (8bit):	5.970149697517944
Encrypted:	false
SSDEEP:	3:yionv//thPl9vtt+NTl0qRthwkBDsTBZtqmA73Fs+rQx33npdtnoypZh9Dicl2up:6v/lhPmNp0WnDspBAzqPnpdiyTh9Fp
MD5:	023F5AC6E0114AF1F781BE5D3C956385
SHA1:	C166284B8541F1DE32DC5C4DEC635C296BF85C98
SHA-256:	75D637BF6B6DFF2525095D0BE7E0C90F012BB118C2EF19099AFDCBC630ADFC79
SHA-512:	DAFA49056E3D3014DB392410685CC05773C09938E2E700657727928EDCFF8EA2D7C769D377539C52DA70321B94F4E8F045F565EC51BC2B701D95BB3213CC220
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/print-icon.png?version=60ebb5de-511c-db20-3795-563c739c5e12
Preview:	.PNG.....IHDR.....h6....tEXtSoftware.Adobe ImageReadyq.e<...OIDATx.b...?..0222`..jX..a5...D0.50.....k.....:...X=....'..(..I.....K..... .....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\privacy-in-our-products[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	69022
Entropy (8bit):	5.216083228802393
Encrypted:	false
SSDEEP:	768:veBUE5N6uHHyKTFKSsKQgGsDkLkEuFEoW1G9ottIliGicPRuDdueyaaFpdaHqGQN:veBUEP6WykQQ
MD5:	F468C213CA92C8F8934BE01A74520515
SHA1:	5FEB1F5EB42F6F911557AB9FD7AC2E64BB9B7271
SHA-256:	3853D867B6719A75602A8D54F0E2F8F938E775F3EABD33C9E3712CEEFA4242C4
SHA-512:	81CE8389D086AAB881061DCF8AEA9A70C26DAAD47B9FE6476C50C218A458E4A9D109A25BEB39B12C8B6A1737B8B97A9722F238EE3B934703108B04FBD3914280
Malicious:	false
Reputation:	low
Preview:	.<!DOCTYPE html ><html xmlns:mscom="http://schemas.microsoft.com/CMSvNext" xmlns:md="http://schemas.microsoft.com/mscom-data" lang="en-us" xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta charset="utf-8" /><meta name="viewport" content="width=device-width, initial-scale=1.0" /><link rel="shortcut icon" href="//www.microsoft.com/favicon.ico?v2" /><script type="text/javascript" src="https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js">.. // Third party scripts and code linked to or referenced from this website are licensed to you by the parties that own such code, not by Microsoft. See ASP.NET Ajax CDN Terms of Use - http://www.asp.net/ajaxlibrary/CDN.ashx... </script><script type="text/javascript" language="javascript">/*<![CDATA[*/if($(document).bind("mobileinit",function(){$.mobile.autoInitializePage=!1}),navigator.userAgent.match(/IEMobile\/10\.0/)){var msViewportStyle=document.createElement("style");msViewpor

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\privacystatement[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	328278

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\privacystatement[1].htm	
Entropy (8bit):	4.8479477411044725
Encrypted:	false
SSDEEP:	3072:nz6s811xiaNyN2d69v36WHkAd5C6ZNRrufSylxqzEZC/Bd7ZENOxCQyZCqTeHwxC:ncxiM6TYs3Nu8iN1yZCSeHaagw
MD5:	9122B7AD0FBB36352A7343789B279B7F
SHA1:	8267DF6DA3A1177C3A08C55E551BC707A71441B9
SHA-256:	3B6934BE800C3FAA28EDC295574B95F1DBA970E5D33509DD04C980D96522891C
SHA-512:	5339B7B3F1F158520DEABEEAB5DFAADC86411422EC1E923AD97C4F5852BF47D034941CF9115F194A5AF0841CB949D8A756E56B597F19D65E750C86E1116AAA1E
Malicious:	false
Reputation:	low
Preview:	.<!DOCTYPE html ><html xmlns:mscom="http://schemas.microsoft.com/CMSvNext" xmlns:md="http://schemas.microsoft.com/mscom-data" lang="en-us" xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta charset="utf-8" /><meta name="viewport" content="width=device-width, initial-scale=1.0" /><link rel="shortcut icon" href="https://www.microsoft.com/favicon.ico?v2" /><script type="text/javascript" src="https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js">...../// Third party scripts and code linked to or referenced from this website are licensed to you by the parties that own such code, not by Microsoft. See ASP.NET Ajax CDN Terms of Use - http://www.asp.net/ajaxlibrary/CDN.ashx... </script><script type="text/javascript" language="javascript">/*<![CDATA[*/if($(document).bind("mobileinit",function(){$.mobile.autoInitializePage=!1}),navigator.userAgent.match(/IEMobile\/10\.0/)){var msViewportStyle=document.createElement("style");msViewpo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\script[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):	30173
Entropy (8bit):	5.326896118392395
Encrypted:	false
SSDEEP:	384:ekorlyUMfQ8sW5hXDiWiQRKKwoOdo/r4nqdRy/dRyWhtyFhtyYKQys05DU7BS5hN:0olDi2RKQOOwqjE2l/3FJ1C/nrjYiKq
MD5:	F620D4D38655075DF3268D640BF479BD
SHA1:	79BEBF5E6907D4CDD5764B9B9CF3A72932F9C343
SHA-256:	7E1377CD02DAFE245ED719FCA972C5E8CFDE30CBF3910D2795A922BB466D08C2
SHA-512:	1A8528BDEEECEB75766B8ACCD7B5DBFE7E45E72A3E52108D3F63C0667ABF1492FBAFDD6F80E9639339BE5EE5C1E4A7B7BCA635C6DBBBEC83044FBC842C37FFCC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=42ce545a-d075-ac8e-38d1-8d9b4eaa1c7e
Preview:	function ShowSelectedComponentKeyPress(n,t){if(window.event.keyCode==13)return ShowSelectedComponent(n,t),!1}function SetRightSideNavigationMenuHeight(){$("[id^=dvModuleGroup_]").hide();window.location.search.toLowerCase().indexOf("bookmarkid")!=-1&&SelectBookMark();window.location.search.toLowerCase().indexOf("componentid")!=-1&&LoadSelectedInternalLink();$(".div_side_comp").length>0&&$(".div_content").css("min-height",$(".div_side_comp").height()-27)}function ShowSelectedComponent(n,t){var i=$("#"+t).attr("data-parentModule");return i!=undefined&&i!=null&&($("[data-parentmodule="+i+"]").show(),$("#"+i+" [id$=_LongDescription]").length>0?(document.getElementById(i+"_LongDescription").style.display="block",document.getElementById(i+"_ShortDescription").style.display="none",ShowText($("#"+i+".learnMoreLabel"),"long")):ShowText($("#"+i+".learnMoreLabel"),"long"),DisplayTopNavigation(i)),$("html, body").animate({scrollTop:$("#"+t).offset().top-1},800),!1}function ShowToolTip(){var n,i,t;w

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\script[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	23352
Entropy (8bit):	5.225460068118695
Encrypted:	false
SSDEEP:	384:IAm+fEydfW5DBs68PycH3vMSZras8PPaW6VufSFTb+BifBFXluVUovZVwDMhAaL/:bffAVcufKTb+QuhVwwhATrG9LaUZV5Im
MD5:	D772996B25001C338CB573795E41253E
SHA1:	BC93DA543536AE3F9F259B7F420D56FBC9CFBFFB
SHA-256:	99411C1003352059F75965F338C95BA0B5B62C47FB5EF9092E2AA249503FD78E
SHA-512:	59DF35F226014FDA10F7A399434D86773C17E7453C02FC61F8429BF79F0D1300C9D87AE2963E4FFED700B873B55BAD12D75E5654382BE3576EA10801BDB2F387
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=17e9fd93-8142-d2e5-0026-505db3628325_1545a2a3-f8ee-1941-5c04-a4b822c95e2c_badc3012-6391-ec2a-3c4d-eda492f079fc_c5ea3348-55af-729a-2641-14f0312bacf3_742bd11f-3d7c-9955-3df5-f02b66689699_5c27e8aa-9347-969e-39ac-37a4de428a8d
Preview:	$(document).ready(function(){var u=536,f=0,e=u,i=0,n,r;$(window).scroll(function(){f=$("#footerArea").length?$("#footerArea").position().top:$(".shell-footer").position().top;e=$(window).scrollTop();i=e+u-f;e>u&&i<0?$(".scrollingBox").css({position:"fixed",top:"15px","margin-top":"0px"}):i>0?$(".scrollingBox").css("margin-top",0-i):$(".scrollingBox").css({position:"static","margin-top":"0px"})});n=$('meta[name="MscomContentLocale"]').attr("content").toLowerCase();document.dir=n=="fa-ir"||n=="he-il"||n=="ku-arab-iq"||n=="pa-arab-pk"||n=="prs-af"||n=="sd-arab-pk"||n=="ug-cn"||n=="ur-pk"||n.substring(0,3)=="ar-"?"rtl":"ltr";n!="en-us"&&$("[market='en-US']").remove();var t=window.location.pathname.replace("/privacy.microsoft.com","").replace("/en-us/","").toLowerCase(),o=t.lastIndexOf("/")+1,s=t.length;t=t.substr(o,s);r=$('nav a[href="'+t+'"i]');r.css("color","grey");r.attr("href","#");r.click(function(n){n.preventDefault()})});./*!.Waypoints - 4.0.1.Copyright . 2011-2016 Caleb Troughton.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\site-oneui[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\site-oneui[1].css	
Category:	downloaded
Size (bytes):	137818
Entropy (8bit):	5.087444856846427
Encrypted:	false
SSDEEP:	3072:SG9qB4aAjGXHsU0Y4wQwKKKsyJySmR4fLq8yP31q8yUiPAniKADjpF19MB1d119c:SG9qB4aAj+tG
MD5:	54F73122B87D956E1267DEB1F4906745
SHA1:	D51AD4E95A8CB836F750E3178FF3402FA44C472F
SHA-256:	BB9C21D19344D3457FC9E8E91FE776B3F6F418D63364EFC312BC95DD5C4FDC20
SHA-512:	5A021EC98A52F10A1B0478AABA8A71FE486C73574D87F6CD03E2F8A54CAC4F9F24C50DACB6144C884668BB85115B6FAE4FC4FF147955EC4064EE5697A0DE930 E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://account.microsoft.com/bundles/styles/site-oneui?v=Oeeg1hhThLQ0Bs49suFEQXph08AXwX2UvzOdVq2g2bs1
Preview:	ol,ul{padding:0;margin:0;list-style:none}.hidden{display:none}@-webkit-viewport{width:device-width;}@-moz-viewport{width:device-width;}@-ms-viewport{width:device-width;}@-o-viewport{width:device-width;}@viewport{width:device-width;}.progress{background-image:none!important}@font-face{font-family:"Dev Center MDL2 Assets";src:url("/Resources/Fonts/DevCMDL2.1.43.eot");src:local("Dev Center MDL2 Assets"),url("/Resources/Fonts/DevCMDL2.1.43.eot?#iefix") format("embedded-opentype"),url("/Resources/Fonts/DevCMDL2.1.43.woff") format("woff"),url("/Resources/Fonts/DevCMDL2.1.43.ttf") format("truetype"),url("/Resources/Fonts/DevCMDL2.1.43.svg#Dev Center MDL2 Assets") format("svg")}.win-icon-Info:before{content:"."}.win-icon-Cancel:before{content:"."}.win-icon-Warning::before{content:"."}.win-icon-CheckMark::before{content:"."}.win-icon-TaskStateCircleFull::before{content:"."}.win-icon-TaskStateComplete::before{content:"."}.win-icon-TaskStateNotStarted::before{content:"."}@media(max-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\site[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	131996
Entropy (8bit):	5.3169457893589716
Encrypted:	false
SSDEEP:	1536:jloFM2JfgcRF9h0KpR3E78Jm8Ld8g3SgWHFBF1x79xikk//W3197t0EDKQqdF+2s:KD2DBF1m/W3197t0EDkdF+Tq8
MD5:	7D8FA8FAEC0524151ED31BDC6C26AA16
SHA1:	3CA9212C23A97BF085E1F8C19DF8D900B1598179
SHA-256:	9A8FF739EC33F96D8D0AA5603B856AA5A4D0B66F19A1BA31825464E92A5845EA
SHA-512:	5A8772C65FAD064F6CC39D31A3F482344024AE24DD10B4BC09AAEA7A8D144F7B357E557A52A4900E6B79D775B86C01135C94A005B82F5F9C0D025B6450E7B44
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://account.microsoft.com/bundles/scripts/site?v=vDloEEMna0v0bDOvhg3Wu9-5aomWGcLr7BbgT0gTGfk1
Preview:	function bingMapLoaded(){MeePortal.BingMapWaiter.mapsLoaded()}var Helpers,inputWidth,mq,WebHip,MeePortal;(function(n,t){typeof exports=="object"&&typeof module!="undefined"?t(exports):typeof define=="function"&&define.amd?define(["exports"],t):t(n.cookieManager=n.cookieManager||{})})(this,function(n){"use strict";function o(n){return n.replace(e,"")}var u=63072e6,t=window,i=window,r=function(){function n(n){var u=this,t,i,r;this.localDocument=n;this.nonEssentialCookies=[];this.previouslyConsentedCookies=[];this.isMsccCallbackRegistered=!1;this.isWCPCallbackRegistered=!1;this.isInFlightGCookieBanner=!1;r=(i=(t=window.MeePortal)===null||t===void 0?void 0:t.g_userFlights)!==null&&i!==void 0?i:[];r.forEach(function(n){n.toLowerCase()==="gcookiebanner"&&(u.isInFlightGCookieBanner=!0)})}return n.prototype.getCookie=function(n,t,i){var e,r,u;if(!n)throw new Error("CookieManager.getCookie - name argument should not be false-y");if(this.isInFlightGCookieBanner&&this.registerWCPCallback(),t&&!th

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\social[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	524838
Entropy (8bit):	4.993034695686957
Encrypted:	false
SSDEEP:	3072:GAwmeEZACGwzyP5kTP3bI0tfYqQ0xtLfj4ZDa813giY8R1j35Ap7zzN1n1JKfNkF:CEZACKmj
MD5:	E23FB35ADA4C463D9CA93850296B303B
SHA1:	474F6B204DDBF63554946B72B1D3D9F4FF6AC5AD
SHA-256:	3CCC51958543B93E842D438EB7E03A1227E54759095750061EEFBE086F7857AA
SHA-512:	4E41D95F146C0CFEBCFE37A703E743D1DD11D1E409FEE8B2A08B23AAA00024AC6652B9554251D9F0DEA3358103B10A96207393483B6FF197023826860FB1BAD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/mwf/css/MWF_20201028_28422223/west-european/default/alert/ambientvideo/areaheading/autosuggest/button/calltoaction/dialog/divider/feature/glyph/heading/hero/heroitem/hyperlinkgroup/image/imageintro/list/logo/mosaic/mosaicplacement/multislidecarousel/pagebehaviors/rating/skiptomain/social?apiVersion=1.0&include_base=true
Preview:	@charset "UTF-8";./*! 1.57.0 | Copyright 2017 Microsoft Corporation | This software is based on or incorporates material from the files listed below (collectively, "Third Party Code"). Microsoft is not the original author of the Third Party Code. The original copyright notice and the license under which Microsoft received Third Party Code are set forth below together with the full text of such license. Such notices and license are provided solely for your information. Microsoft, not the third party, licenses this Third Party Code to you under the terms in which you received the Microsoft software or the services, unless Microsoft clearly states that such Microsoft terms do NOT apply for a particular Third Party Code. Unless applicable law gives you more rights, Microsoft reserves all other rights not expressly granted under such agreement(s), whether by implication, estoppel or otherwise.*/./*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */.html{font-family:sa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	836
Entropy (8bit):	4.940950417710206
Encrypted:	false
SSDEEP:	24:Cn5ZoK2kNMCJZ4ZVaeao1DphsILHJNM2WXgEXgf0Xgm:u5dxJZ4+BWIIPLQ73/
MD5:	2AC383F4677A1036C8EA4289F99A31E3
SHA1:	E65967B9273029CDDD5A5F8DF9E61DACF89CF11C
SHA-256:	2206A95E6BAC7C185CC54638EBF0B0089CBC27FF729B45AC63C968CFE4991AA4
SHA-512:	9E61D4E2B42A1BC776C5649ECD2E32A1CE1ACEDA929E8C013D20BE95D12B7B56864FD588D6117E6410988331F85E21815E2E135030F49BEA2A244F872570DBE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSStyles/style.csx?k=4627136a-bd68-db6e-30c9-37cf96c98eee
Preview:	body .grid,.body-open .grid,.grid h3,.grid .h3,.grid .header-small,.grid strong,.grid .body-tight-2,.grid h1,.grid .h1,.grid .header-large,.grid .caption{font-family:"Segoe UI"}.grid{max-width:1600px !important}.c-uhfh-actions,.c-uhfh-gcontainer-st .all-ms-nav,.glyph-global-nav-button{display:none !important}.shell-header-wrapper,.shell-footer-wrapper,.shell-category-nav,.shell-notification .shell-notification-grid-row{max-width:1180px !important}.PsTitle{font-family:Segoe UI,sans-serif;margin-right:.3em !important;font-size:2em;display:inline-block;vertical-align:top;margin-left:-.02em}.childModule{margin-left:8% !important}.CollectingYourInfoRightNav{display:none}html[dir=rtl] .m-r-md{margin-right:0;margin-left:10px}html[dir=rtl] .m-l-md{margin-left:0;margin-right:10px}html[dir=rtl] .m-r-bl{margin-right:0;margin-left:40px}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\surface[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	161377
Entropy (8bit):	5.343053727021629
Encrypted:	false
SSDEEP:	1536:/BEroKoaR4qHTHWlMWe30txV8UMd/U0ql30C49ud:/SUKoaR4qHT2DEdtNC49m
MD5:	15418538D7BE6414C8516A5751C9A142
SHA1:	B1F1D67DF1633356CF1B74159CA0CFE71418A3EE
SHA-256:	855A26C5C1093D3A3BD7041A00BDF60ED3F4E83B18ADC5ADF1794A2CD5103CDE
SHA-512:	846277CD95F1F3F0376D6EFA52507B66EF47CDEB91C4AF23EF528341FAEC5A7850F3F133CEE71B2C498804CC552B92D3DABE4ABD2A1C5EFA5415898D86813B0
Malicious:	false
Reputation:	low
Preview:	.<!DOCTYPE html ><html xmlns:mscom="http://schemas.microsoft.com/CMSvNext" xmlns:md="http://schemas.microsoft.com/mscom-data" class="grunticon skrollr skrollr-desktop" lang="en-us" xmlns="http://www.w3.org/1999/xhtml"><head> <meta content="width=device-width, initial-scale=1.0" name="viewport" /--> <mscom:conditional propertyexists="true" instancename="isCookieConsentRequired" customexpression="False::False"--> <script type="text/javascript" src="//www.microsoft.com/library/svy/min/pre_broker.js" async="true"></script>...<script type="text/javascript" src="//www.microsoft.com/library/svy/min/broker.js" async="true"></script--> </mscom:conditional>--><meta charset="utf-8" /><meta content="IE=edge,chrome=1" http-equiv="X-UA-Compatible" /><meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=5.0" /><link rel="shortcut icon" href="//www.microsoft.com/favicon.ico?v2" /><link rel="canonical" href="https://www.microsoft.com/en-us/surface"></link>

Static File Info

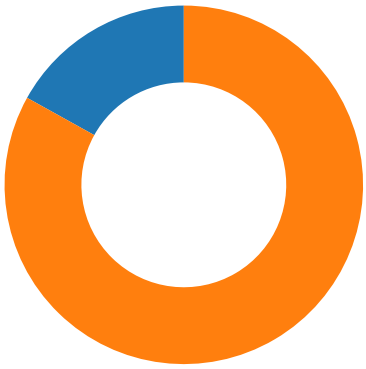
No static file info

Network Behavior

Network Port Distribution

Total Packets: 124

- 53 (DNS)
- 443 (HTTPS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 06:19:51.041024923 CET	49793	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.042123079 CET	49794	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.057180882 CET	443	49793	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.057261944 CET	49793	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.058176994 CET	49793	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.058548927 CET	443	49794	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.058620930 CET	49794	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.059242964 CET	49794	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.074410915 CET	443	49793	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.075292110 CET	443	49793	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.075320005 CET	443	49793	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.075345993 CET	49793	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.075347900 CET	443	49793	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.075367928 CET	443	49793	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.075370073 CET	49793	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.075387955 CET	443	49793	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.075407028 CET	443	49794	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.075407982 CET	49793	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.075433969 CET	49793	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.076894999 CET	443	49794	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.076920986 CET	443	49794	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.076948881 CET	443	49794	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.076951981 CET	49794	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.076967955 CET	443	49794	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.076982975 CET	49794	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.076987982 CET	443	49794	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.077013016 CET	49794	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.077055931 CET	49794	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.091578007 CET	49793	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.091682911 CET	49794	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.092072010 CET	49793	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.092202902 CET	49794	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.092247963 CET	49793	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.108186007 CET	443	49793	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.108223915 CET	443	49793	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.108261108 CET	443	49794	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.108261108 CET	49793	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.108282089 CET	49793	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.108294964 CET	443	49794	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.108326912 CET	443	49793	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.108352900 CET	443	49794	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.108391047 CET	49793	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.108347893 CET	49794	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.108443022 CET	49794	443	192.168.2.4	192.229.221.185

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 06:19:51.108449936 CET	49794	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.109164000 CET	49794	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.109379053 CET	49793	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.109455109 CET	443	49793	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.109496117 CET	443	49793	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.109527111 CET	49793	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.109534025 CET	443	49793	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.109554052 CET	49793	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.109571934 CET	443	49793	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.109592915 CET	49793	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.109610081 CET	443	49793	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.109627962 CET	49793	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.109663963 CET	49793	443	192.168.2.4	192.229.221.185
Nov 26, 2020 06:19:51.166910887 CET	443	49794	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.167124033 CET	443	49793	192.229.221.185	192.168.2.4
Nov 26, 2020 06:19:51.822195053 CET	49801	443	192.168.2.4	23.211.149.25
Nov 26, 2020 06:19:51.822374105 CET	49802	443	192.168.2.4	23.211.149.25
Nov 26, 2020 06:19:51.841649055 CET	443	49801	23.211.149.25	192.168.2.4
Nov 26, 2020 06:19:51.841697931 CET	443	49802	23.211.149.25	192.168.2.4
Nov 26, 2020 06:19:51.841782093 CET	49801	443	192.168.2.4	23.211.149.25
Nov 26, 2020 06:19:51.841798067 CET	49802	443	192.168.2.4	23.211.149.25
Nov 26, 2020 06:19:51.842814922 CET	49801	443	192.168.2.4	23.211.149.25
Nov 26, 2020 06:19:51.842865944 CET	49802	443	192.168.2.4	23.211.149.25
Nov 26, 2020 06:19:51.862447977 CET	443	49802	23.211.149.25	192.168.2.4
Nov 26, 2020 06:19:51.862461090 CET	443	49801	23.211.149.25	192.168.2.4
Nov 26, 2020 06:19:51.863892078 CET	443	49801	23.211.149.25	192.168.2.4
Nov 26, 2020 06:19:51.863919020 CET	443	49801	23.211.149.25	192.168.2.4
Nov 26, 2020 06:19:51.863940001 CET	443	49801	23.211.149.25	192.168.2.4
Nov 26, 2020 06:19:51.863954067 CET	443	49801	23.211.149.25	192.168.2.4
Nov 26, 2020 06:19:51.863970995 CET	443	49802	23.211.149.25	192.168.2.4
Nov 26, 2020 06:19:51.863982916 CET	49801	443	192.168.2.4	23.211.149.25
Nov 26, 2020 06:19:51.863987923 CET	443	49802	23.211.149.25	192.168.2.4
Nov 26, 2020 06:19:51.864002943 CET	49801	443	192.168.2.4	23.211.149.25
Nov 26, 2020 06:19:51.864005089 CET	443	49802	23.211.149.25	192.168.2.4
Nov 26, 2020 06:19:51.864017010 CET	443	49802	23.211.149.25	192.168.2.4
Nov 26, 2020 06:19:51.864026070 CET	49801	443	192.168.2.4	23.211.149.25
Nov 26, 2020 06:19:51.864031076 CET	49802	443	192.168.2.4	23.211.149.25
Nov 26, 2020 06:19:51.864063978 CET	49802	443	192.168.2.4	23.211.149.25
Nov 26, 2020 06:19:51.883414984 CET	443	49802	23.211.149.25	192.168.2.4
Nov 26, 2020 06:19:51.883440018 CET	443	49801	23.211.149.25	192.168.2.4
Nov 26, 2020 06:19:51.883496046 CET	49802	443	192.168.2.4	23.211.149.25
Nov 26, 2020 06:19:51.883533001 CET	49801	443	192.168.2.4	23.211.149.25
Nov 26, 2020 06:19:51.887346983 CET	49801	443	192.168.2.4	23.211.149.25
Nov 26, 2020 06:19:51.888020992 CET	49801	443	192.168.2.4	23.211.149.25
Nov 26, 2020 06:19:51.892455101 CET	49802	443	192.168.2.4	23.211.149.25
Nov 26, 2020 06:19:51.906793118 CET	443	49801	23.211.149.25	192.168.2.4
Nov 26, 2020 06:19:51.907036066 CET	443	49801	23.211.149.25	192.168.2.4
Nov 26, 2020 06:19:51.907103062 CET	49801	443	192.168.2.4	23.211.149.25
Nov 26, 2020 06:19:51.907365084 CET	443	49801	23.211.149.25	192.168.2.4
Nov 26, 2020 06:19:51.911813974 CET	443	49802	23.211.149.25	192.168.2.4
Nov 26, 2020 06:19:51.913968086 CET	443	49801	23.211.149.25	192.168.2.4
Nov 26, 2020 06:19:51.914058924 CET	49801	443	192.168.2.4	23.211.149.25
Nov 26, 2020 06:19:51.915424109 CET	443	49802	23.211.149.25	192.168.2.4
Nov 26, 2020 06:19:51.915501118 CET	49802	443	192.168.2.4	23.211.149.25
Nov 26, 2020 06:20:08.324481010 CET	49823	443	192.168.2.4	52.239.152.74
Nov 26, 2020 06:20:08.326361895 CET	49824	443	192.168.2.4	52.239.152.74

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 06:19:03.655472040 CET	62389	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:03.691061974 CET	53	62389	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:05.043745995 CET	49910	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:05.079468966 CET	53	49910	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 06:19:07.471682072 CET	55854	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:07.508760929 CET	53	55854	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:07.776108980 CET	64549	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:07.803369045 CET	53	64549	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:08.446474075 CET	63153	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:08.584546089 CET	53	63153	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:08.796252012 CET	52991	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:08.831856966 CET	53	52991	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:10.046161890 CET	53700	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:10.056938887 CET	51726	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:10.085338116 CET	53	53700	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:10.093871117 CET	53	51726	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:10.567868948 CET	56794	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:10.603200912 CET	53	56794	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:12.720237970 CET	56534	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:12.755956888 CET	53	56534	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:13.770277977 CET	56627	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:13.808330059 CET	53	56627	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:16.906943083 CET	56621	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:16.934093952 CET	53	56621	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:17.718750954 CET	63116	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:17.754435062 CET	53	63116	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:18.395695925 CET	64078	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:18.431174994 CET	53	64078	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:19.410430908 CET	64801	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:19.445921898 CET	53	64801	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:20.228919983 CET	61721	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:20.264648914 CET	53	61721	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:20.896313906 CET	51255	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:20.923666000 CET	53	51255	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:24.797075033 CET	61522	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:24.894467115 CET	53	61522	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:26.088083982 CET	52337	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:26.124022961 CET	53	52337	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:27.004185915 CET	55046	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:27.047991991 CET	53	55046	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:27.820391893 CET	49612	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:27.849154949 CET	53	49612	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:28.339204073 CET	49285	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:28.366328955 CET	53	49285	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:37.471985102 CET	50601	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:37.510818005 CET	53	50601	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:38.152226925 CET	60875	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:38.188049078 CET	53	60875	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:38.479134083 CET	50601	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:38.515018940 CET	53	50601	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:38.592984915 CET	56448	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:38.630145073 CET	53	56448	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:38.884602070 CET	59172	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:38.921781063 CET	53	59172	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:39.160995960 CET	60875	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:39.196697950 CET	53	60875	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:39.480915070 CET	62420	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:39.484210968 CET	60579	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:39.498589993 CET	50601	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:39.521508932 CET	53	60579	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:39.528301954 CET	53	62420	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:39.534307003 CET	53	50601	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:39.543313026 CET	50183	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:39.545768023 CET	61531	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:39.551032066 CET	49228	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:39.580127001 CET	53	50183	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:39.582734108 CET	53	61531	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:39.584908009 CET	59794	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 06:19:39.589010954 CET	53	49228	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:39.621932030 CET	53	59794	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:40.188148975 CET	60875	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:40.223866940 CET	53	60875	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:41.440242052 CET	55916	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:41.477343082 CET	53	55916	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:41.510516882 CET	50601	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:41.546272039 CET	53	50601	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:42.198060989 CET	60875	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:42.233593941 CET	53	60875	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:43.215187073 CET	52752	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:43.250993013 CET	53	52752	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:45.510766029 CET	50601	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:45.546340942 CET	53	50601	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:45.769490004 CET	60542	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:45.806240082 CET	53	60542	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:46.200800896 CET	60875	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:46.236264944 CET	53	60875	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:47.040050030 CET	60689	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:47.079411030 CET	53	60689	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:47.458370924 CET	64206	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:47.497323036 CET	53	64206	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:48.865031958 CET	50904	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:48.865674019 CET	57525	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:48.871433973 CET	53814	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:48.900602102 CET	53418	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:48.901623011 CET	53	50904	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:48.902182102 CET	53	57525	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:48.907351971 CET	53	53814	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:48.937674999 CET	53	53418	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:49.898493052 CET	62833	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:49.949539900 CET	53	62833	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:50.652129889 CET	59260	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:50.762923002 CET	53	59260	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:50.762953997 CET	49944	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:50.805813074 CET	53	49944	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:50.986963987 CET	63300	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:51.039371014 CET	53	63300	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:51.278845072 CET	61449	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:51.314501047 CET	53	61449	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:51.616072893 CET	51275	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:51.651853085 CET	53	51275	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:51.792031050 CET	63492	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:51.819202900 CET	53	63492	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:52.035999060 CET	58945	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:52.071773052 CET	53	58945	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:54.280749083 CET	60779	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:54.331553936 CET	53	60779	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:54.984504938 CET	64014	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:55.020407915 CET	53	64014	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:55.781178951 CET	57091	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:55.808418036 CET	53	57091	8.8.8.8	192.168.2.4
Nov 26, 2020 06:19:59.295286894 CET	55904	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:19:59.330936909 CET	53	55904	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:00.178345919 CET	52109	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:00.213896990 CET	53	52109	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:00.726670980 CET	54450	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:00.762355089 CET	53	54450	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:03.282879114 CET	49374	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:03.321754932 CET	53	49374	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:03.523262978 CET	50436	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:03.560214996 CET	53	50436	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:06.330809116 CET	62605	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:06.341310024 CET	54256	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 06:20:06.369975090 CET	53	62605	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:06.378163099 CET	53	54256	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:06.388859034 CET	52189	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:06.426337957 CET	53	52189	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:08.231525898 CET	56131	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:08.243850946 CET	62992	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:08.279334068 CET	53	62992	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:08.305670977 CET	53	56131	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:09.245372057 CET	62992	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:09.280978918 CET	53	62992	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:10.249594927 CET	62992	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:10.285157919 CET	53	62992	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:12.255496025 CET	62992	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:12.290862083 CET	53	62992	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:12.396677017 CET	54432	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:12.440036058 CET	53	54432	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:12.524605036 CET	57227	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:12.568519115 CET	53	57227	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:12.698689938 CET	58383	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:12.728235006 CET	53	58383	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:13.704901934 CET	63136	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:13.741919994 CET	53	63136	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:13.996632099 CET	50911	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:14.009258032 CET	63409	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:14.034463882 CET	53	50911	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:14.046386003 CET	53	63409	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:14.524928093 CET	59185	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:14.552285910 CET	53	59185	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:16.628703117 CET	62992	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:16.664551973 CET	53	62992	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:16.861118078 CET	64236	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:16.900082111 CET	53	64236	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:18.775783062 CET	56157	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:18.812844992 CET	53	56157	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:19.056472063 CET	55601	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:19.065598965 CET	52984	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:19.094284058 CET	53	55601	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:19.105185032 CET	53	52984	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:19.816622972 CET	51141	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:19.828917027 CET	61247	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:19.829371929 CET	53610	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:19.856261969 CET	53	51141	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:19.864658117 CET	53	61247	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:19.878985882 CET	53	53610	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:20.293524981 CET	65165	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:20.364718914 CET	53	65165	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:21.221324921 CET	52076	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:21.231368065 CET	54903	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:21.232584000 CET	55045	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:21.232974052 CET	54464	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:21.233458042 CET	50970	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:21.256582975 CET	53	52076	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:21.269229889 CET	53	55045	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:21.270143986 CET	53	54903	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:21.270215988 CET	53	50970	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:21.275938988 CET	53	54464	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:25.692426920 CET	55261	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:25.729475975 CET	53	55261	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:29.128370047 CET	59809	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:29.131820917 CET	51278	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:29.142910957 CET	51932	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:29.166634083 CET	53	59809	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:29.175602913 CET	53	51278	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:29.180393934 CET	53	51932	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 06:20:29.202465057 CET	59494	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:29.204770088 CET	55915	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:29.224127054 CET	49779	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:29.247390032 CET	53	59494	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:29.260878086 CET	49458	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:29.261328936 CET	53	49779	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:29.262092113 CET	57164	53	192.168.2.4	8.8.8.8
Nov 26, 2020 06:20:29.270831108 CET	53	55915	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:29.297663927 CET	53	57164	8.8.8.8	192.168.2.4
Nov 26, 2020 06:20:29.300179005 CET	53	49458	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 26, 2020 06:19:08.446474075 CET	192.168.2.4	8.8.8.8	0xcb5d	Standard query (0)	pembina.sharepoint.com	A (IP address)	IN (0x0001)
Nov 26, 2020 06:19:10.056938887 CET	192.168.2.4	8.8.8.8	0xe15	Standard query (0)	spoprod-a.akamaihd.net	A (IP address)	IN (0x0001)
Nov 26, 2020 06:19:24.797075033 CET	192.168.2.4	8.8.8.8	0x5e42	Standard query (0)	pembina.sharepoint.com	A (IP address)	IN (0x0001)
Nov 26, 2020 06:19:39.480915070 CET	192.168.2.4	8.8.8.8	0xf58	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Nov 26, 2020 06:19:39.551032066 CET	192.168.2.4	8.8.8.8	0xce55	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)
Nov 26, 2020 06:19:48.900602102 CET	192.168.2.4	8.8.8.8	0x273a	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)
Nov 26, 2020 06:19:50.986963987 CET	192.168.2.4	8.8.8.8	0x3031	Standard query (0)	logincdn.msauth.net	A (IP address)	IN (0x0001)
Nov 26, 2020 06:19:51.792031050 CET	192.168.2.4	8.8.8.8	0xae3e	Standard query (0)	aka.ms	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:03.523262978 CET	192.168.2.4	8.8.8.8	0x5488	Standard query (0)	amp.azure.net	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:06.341310024 CET	192.168.2.4	8.8.8.8	0xfe28	Standard query (0)	assets.adobedtm.com	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:08.231525898 CET	192.168.2.4	8.8.8.8	0x54cb	Standard query (0)	offertoolodataprod.blob.core.windows.net	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:12.396677017 CET	192.168.2.4	8.8.8.8	0xb341	Standard query (0)	consentreceiverfd-prod.azurefd.net	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:13.704901934 CET	192.168.2.4	8.8.8.8	0x868c	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:13.996632099 CET	192.168.2.4	8.8.8.8	0xa6d9	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:14.009258032 CET	192.168.2.4	8.8.8.8	0x5dde	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:14.524928093 CET	192.168.2.4	8.8.8.8	0x9339	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:16.861118078 CET	192.168.2.4	8.8.8.8	0x6e6f	Standard query (0)	cdn.optimizely.com	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:18.775783062 CET	192.168.2.4	8.8.8.8	0x197	Standard query (0)	mscom.demdex.net	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:19.056472063 CET	192.168.2.4	8.8.8.8	0xd9d4	Standard query (0)	api.company-target.com	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:19.065598965 CET	192.168.2.4	8.8.8.8	0xa93b	Standard query (0)	dpm.demdex.net	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:19.816622972 CET	192.168.2.4	8.8.8.8	0x2362	Standard query (0)	ct.pinterest.com	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:19.828917027 CET	192.168.2.4	8.8.8.8	0xc487	Standard query (0)	logx.optimizely.com	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:19.829371929 CET	192.168.2.4	8.8.8.8	0x2457	Standard query (0)	a3698060313.cdn.optimizely.com	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:20.293524981 CET	192.168.2.4	8.8.8.8	0x43f6	Standard query (0)	surfaceselfserviceoffertool.azurewebsites.net	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:21.231368065 CET	192.168.2.4	8.8.8.8	0x67cc	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:21.232974052 CET	192.168.2.4	8.8.8.8	0xf0a3	Standard query (0)	microsoftwindows.112.2o7.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 26, 2020 06:20:21.233458042 CET	192.168.2.4	8.8.8.8	0xc6c	Standard query (0)	assets.one store.ms	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:29.128370047 CET	192.168.2.4	8.8.8.8	0x92c9	Standard query (0)	assets.one store.ms	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:29.142910957 CET	192.168.2.4	8.8.8.8	0xea31	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:29.202465057 CET	192.168.2.4	8.8.8.8	0x598	Standard query (0)	statics-wc us.onestore.ms	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:29.204770088 CET	192.168.2.4	8.8.8.8	0xb218	Standard query (0)	statics-eu s.onestore.ms	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:29.224127054 CET	192.168.2.4	8.8.8.8	0xd4af	Standard query (0)	statics-ea s.onestore.ms	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:29.260878086 CET	192.168.2.4	8.8.8.8	0x427d	Standard query (0)	statics-ne u.onestore.ms	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 06:19:08.584546089 CET	8.8.8.8	192.168.2.4	0xcb5d	No error (0)	pembina.sh arepoint.com	688-ipv4e.clump.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:19:08.584546089 CET	8.8.8.8	192.168.2.4	0xcb5d	No error (0)	688-ipv4e. clump.prod.aa-rt.sharepoint.com	18979-ipv4e.farm.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:19:08.584546089 CET	8.8.8.8	192.168.2.4	0xcb5d	No error (0)	18979-ipv4 e.farm.prod.aa-rt.sharepoint.com	18979-ipv4e.farm.prod.sharepointonline.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:19:10.093871117 CET	8.8.8.8	192.168.2.4	0xe15	No error (0)	spoprod-a. akamaihd.net	spoprod-a.akamaihd.net.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:19:24.894467115 CET	8.8.8.8	192.168.2.4	0x5e42	No error (0)	pembina.sh arepoint.com	688-ipv4e.clump.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:19:24.894467115 CET	8.8.8.8	192.168.2.4	0x5e42	No error (0)	688-ipv4e. clump.prod.aa-rt.sharepoint.com	18979-ipv4e.farm.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:19:24.894467115 CET	8.8.8.8	192.168.2.4	0x5e42	No error (0)	18979-ipv4 e.farm.prod.aa-rt.sharepoint.com	18979-ipv4e.farm.prod.sharepointonline.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:19:39.528301954 CET	8.8.8.8	192.168.2.4	0xf58	No error (0)	ajax.aspne tcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:19:39.589010954 CET	8.8.8.8	192.168.2.4	0xce55	No error (0)	assets.one store.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:19:47.497323036 CET	8.8.8.8	192.168.2.4	0x5042	No error (0)	prda.aadg. msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:19:48.907351971 CET	8.8.8.8	192.168.2.4	0x44dc	No error (0)	consentdel iveryfd.az urefd.net	star-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:19:48.937674999 CET	8.8.8.8	192.168.2.4	0x273a	No error (0)	mem.gfx.ms	cdn.account.microsoft.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:19:51.039371014 CET	8.8.8.8	192.168.2.4	0x3031	No error (0)	logincdn.m sauth.net	lgincdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:19:51.039371014 CET	8.8.8.8	192.168.2.4	0x3031	No error (0)	cs1227.wpc .alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)
Nov 26, 2020 06:19:51.819202900 CET	8.8.8.8	192.168.2.4	0xae3e	No error (0)	aka.ms		23.211.149.25	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:03.560214996 CET	8.8.8.8	192.168.2.4	0x5488	No error (0)	amp.azure.net	160c1.wpc.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:06.378163099 CET	8.8.8.8	192.168.2.4	0xfe28	No error (0)	assets.ado bedtm.com	cn-assets.adobedtm.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:08.305670977 CET	8.8.8.8	192.168.2.4	0x54cb	No error (0)	offertoold ataprod.bl ob.core.wi ndows.net	blob.bl6prdstr14a.store.core.windows.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 06:20:08.305670977 CET	8.8.8.8	192.168.2.4	0x54cb	No error (0)	blob.bl6prdstr14a.store.core.windows.net		52.239.152.74	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:12.440036058 CET	8.8.8.8	192.168.2.4	0xb341	No error (0)	consentreceiverfd-prod.azurefd.net	star-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:12.568519115 CET	8.8.8.8	192.168.2.4	0xc3b3	No error (0)	c.msn.com	c-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:13.741919994 CET	8.8.8.8	192.168.2.4	0x868c	No error (0)	snap.licdn.com	wildcard.licdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:14.034463882 CET	8.8.8.8	192.168.2.4	0xa6d9	No error (0)	px.ads.linkedin.com	mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:14.034463882 CET	8.8.8.8	192.168.2.4	0xa6d9	No error (0)	mix.linkedin.com	pop-efr5.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:14.034463882 CET	8.8.8.8	192.168.2.4	0xa6d9	No error (0)	pop-efr5.mix.linkedin.com		185.63.145.5	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:14.046386003 CET	8.8.8.8	192.168.2.4	0x5dde	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:14.046386003 CET	8.8.8.8	192.168.2.4	0x5dde	No error (0)	scontent.xx.fbcdn.net		185.60.216.19	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:14.552285910 CET	8.8.8.8	192.168.2.4	0x9339	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:16.900082111 CET	8.8.8.8	192.168.2.4	0x6e6f	No error (0)	cdn.optimizely.com	cdn.o6.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:18.812844992 CET	8.8.8.8	192.168.2.4	0x197	No error (0)	mscom.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:18.812844992 CET	8.8.8.8	192.168.2.4	0x197	No error (0)	gslb-2.demdex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:18.812844992 CET	8.8.8.8	192.168.2.4	0x197	No error (0)	edge-irl1.demdex.net	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:18.812844992 CET	8.8.8.8	192.168.2.4	0x197	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.248.49.247	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:18.812844992 CET	8.8.8.8	192.168.2.4	0x197	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.241.138.222	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:18.812844992 CET	8.8.8.8	192.168.2.4	0x197	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		3.248.78.233	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:18.812844992 CET	8.8.8.8	192.168.2.4	0x197	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.242.67.216	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:18.812844992 CET	8.8.8.8	192.168.2.4	0x197	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.49.47.228	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:18.812844992 CET	8.8.8.8	192.168.2.4	0x197	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.212.209.68	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:18.812844992 CET	8.8.8.8	192.168.2.4	0x197	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.248.119.134	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:18.812844992 CET	8.8.8.8	192.168.2.4	0x197	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		63.32.152.233	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:19.094284058 CET	8.8.8.8	192.168.2.4	0xd9d4	No error (0)	api.company-target.com		13.224.93.10	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 06:20:19.094284058 CET	8.8.8.8	192.168.2.4	0xd9d4	No error (0)	api.company-target.com		13.224.93.30	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:19.094284058 CET	8.8.8.8	192.168.2.4	0xd9d4	No error (0)	api.company-target.com		13.224.93.47	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:19.094284058 CET	8.8.8.8	192.168.2.4	0xd9d4	No error (0)	api.company-target.com		13.224.93.45	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:19.105185032 CET	8.8.8.8	192.168.2.4	0xa93b	No error (0)	dpm.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:19.105185032 CET	8.8.8.8	192.168.2.4	0xa93b	No error (0)	gslb-2.demdex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:19.105185032 CET	8.8.8.8	192.168.2.4	0xa93b	No error (0)	edge-irl1.demdex.net	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:19.105185032 CET	8.8.8.8	192.168.2.4	0xa93b	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.50.104.129	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:19.105185032 CET	8.8.8.8	192.168.2.4	0xa93b	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.249.66.13	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:19.105185032 CET	8.8.8.8	192.168.2.4	0xa93b	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.19.92.244	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:19.105185032 CET	8.8.8.8	192.168.2.4	0xa93b	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.248.49.247	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:19.105185032 CET	8.8.8.8	192.168.2.4	0xa93b	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.251.184.34	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:19.105185032 CET	8.8.8.8	192.168.2.4	0xa93b	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.212.154.51	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:19.105185032 CET	8.8.8.8	192.168.2.4	0xa93b	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.229.194.56	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:19.105185032 CET	8.8.8.8	192.168.2.4	0xa93b	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		63.32.152.233	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:19.856261969 CET	8.8.8.8	192.168.2.4	0x2362	No error (0)	ct.pinterest.com	www.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:19.856261969 CET	8.8.8.8	192.168.2.4	0x2362	No error (0)	www.pinterest.com	www.pinterest.com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:19.856261969 CET	8.8.8.8	192.168.2.4	0x2362	No error (0)	www.pinterest.com.gslb.pinterest.com	2-01-37d2-0018.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:19.864658117 CET	8.8.8.8	192.168.2.4	0xc487	No error (0)	logx.optimizely.com	p13nlog-1106815646.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:19.864658117 CET	8.8.8.8	192.168.2.4	0xc487	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		50.16.119.144	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:19.864658117 CET	8.8.8.8	192.168.2.4	0xc487	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		35.173.160.60	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:19.864658117 CET	8.8.8.8	192.168.2.4	0xc487	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		34.197.33.90	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 06:20:19.864658117 CET	8.8.8.8	192.168.2.4	0xc487	No error (0)	p13nlog-11 06815646.us-east-1.elb.amazonaws.com		34.197.138.50	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:19.864658117 CET	8.8.8.8	192.168.2.4	0xc487	No error (0)	p13nlog-11 06815646.us-east-1.elb.amazonaws.com		52.20.153.254	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:19.864658117 CET	8.8.8.8	192.168.2.4	0xc487	No error (0)	p13nlog-11 06815646.us-east-1.elb.amazonaws.com		52.44.154.79	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:19.864658117 CET	8.8.8.8	192.168.2.4	0xc487	No error (0)	p13nlog-11 06815646.us-east-1.elb.amazonaws.com		52.86.100.219	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:19.864658117 CET	8.8.8.8	192.168.2.4	0xc487	No error (0)	p13nlog-11 06815646.us-east-1.elb.amazonaws.com		52.205.126.69	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:19.878985882 CET	8.8.8.8	192.168.2.4	0x2457	No error (0)	a3698060313.cdn.optimizely.com	wildcard.cdn.optimizely.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:20.364718914 CET	8.8.8.8	192.168.2.4	0x43f6	No error (0)	surfacesel fserviceof fertool.azurewebsites.net	waws-prod-mwh-031.sip.azurewebsites.windows.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:20.364718914 CET	8.8.8.8	192.168.2.4	0x43f6	No error (0)	waws-prod-mwh-031.sip.azurewebsites.windows.net	waws-prod-mwh-031.cloudapp.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:21.270143986 CET	8.8.8.8	192.168.2.4	0x67cc	No error (0)	mem.gfx.ms	cdn.account.microsoft.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:21.270215988 CET	8.8.8.8	192.168.2.4	0xc6c	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:21.275938988 CET	8.8.8.8	192.168.2.4	0xf0a3	No error (0)	microsoftwindows.112.2o7.net		35.181.18.61	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:21.275938988 CET	8.8.8.8	192.168.2.4	0xf0a3	No error (0)	microsoftwindows.112.2o7.net		15.237.76.117	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:21.275938988 CET	8.8.8.8	192.168.2.4	0xf0a3	No error (0)	microsoftwindows.112.2o7.net		15.237.136.106	A (IP address)	IN (0x0001)
Nov 26, 2020 06:20:29.166634083 CET	8.8.8.8	192.168.2.4	0x92c9	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:29.180393934 CET	8.8.8.8	192.168.2.4	0xea31	No error (0)	mem.gfx.ms	cdn.account.microsoft.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:29.247390032 CET	8.8.8.8	192.168.2.4	0x598	No error (0)	statics-wcus.onestore.ms	statics.onestore.ms.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:29.261328936 CET	8.8.8.8	192.168.2.4	0xd4af	No error (0)	statics-eas.onestore.ms	statics.onestore.ms.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:29.270831108 CET	8.8.8.8	192.168.2.4	0xb218	No error (0)	statics-eus.onestore.ms	statics.onestore.ms.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 06:20:29.300179005 CET	8.8.8.8	192.168.2.4	0x427d	No error (0)	statics-neu.onestore.ms	statics.onestore.ms.edgekey.net		CNAME (Canonical name)	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
Nov 26, 2020 06:19:51.075367928 CET	192.229.221.185	443	192.168.2.4	49793	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jul 20 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Tue Jul 20 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Nov 26, 2020 06:19:51.076967955 CET	192.229.221.185	443	192.168.2.4	49794	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jul 20 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Tue Jul 20 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Nov 26, 2020 06:19:51.863940001 CET	23.211.149.25	443	192.168.2.4	49801	CN=go.microsoft.com, OU=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft IT TLS CA 5, OU=Microsoft IT, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US	CN=Microsoft IT TLS CA 5, OU=Microsoft IT, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Sep 06 21:37:21 CEST 2019 Fri May 20 14:53:03 CEST 2016	Mon Sep 06 21:37:21 CEST 2021 Mon May 20 14:53:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Microsoft IT TLS CA 5, OU=Microsoft IT, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri May 20 14:53:03 CEST 2016	Mon May 20 14:53:03 CEST 2024		
Nov 26, 2020 06:19:51.864005089 CET	23.211.149.25	443	192.168.2.4	49802	CN=go.microsoft.com, OU=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft IT TLS CA 5, OU=Microsoft IT, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US	CN=Microsoft IT TLS CA 5, OU=Microsoft IT, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Sep 06 21:37:21 CEST 2019 Fri May 20 14:53:03 CEST 2016	Mon Sep 06 21:37:21 CEST 2021 Mon May 20 14:53:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Microsoft IT TLS CA 5, OU=Microsoft IT, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri May 20 14:53:03 CEST 2016	Mon May 20 14:53:03 CEST 2024		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 26, 2020 06:20:14.083539009 CET	185.63.145.5	443	192.168.2.4	49832	CN=px.ads.linkedin.com, O=LinkedIn Corporation, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Aug 05 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Fri Feb 05 13:00:00 CET 2021 Wed Mar 08 13:00:00 CET 2023	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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Nov 26, 2020 06:20:14.083760023 CET	185.60.216.19	443	192.168.2.4	49835	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 02 01:00:00 CET 2020 Tue Oct 22 14:00:00 CEST 2013	Sun Jan 31 00:59:59 CET 2021 Sun Oct 22 14:00:00 CEST 2028	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Nov 26, 2020 06:20:14.084121943 CET	185.63.145.5	443	192.168.2.4	49833	CN=px.ads.linkedin.com, O=LinkedIn Corporation, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Aug 05 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Fri Feb 05 13:00:00 CET 2021 Wed Mar 08 13:00:00 CET 2023	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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Nov 26, 2020 06:20:14.089660883 CET	185.60.216.19	443	192.168.2.4	49834	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 02 01:00:00 CET 2020 Tue Oct 22 14:00:00 CEST 2013	Sun Jan 31 00:59:59 CET 2021 Sun Oct 22 14:00:00 CEST 2028	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Nov 26, 2020 06:20:18.893996000 CET	34.248.49.247	443	192.168.2.4	49841	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jan 09 01:00:00 CET 2018 Tue Oct 22 14:00:00 CEST 2013	Fri Feb 12 13:00:00 CET 2021 Sun Oct 22 14:00:00 CEST 2028	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

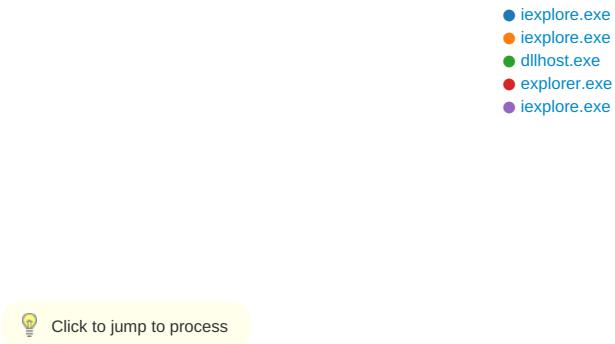
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 26, 2020 06:20:18.894186020 CET	34.248.49.247	443	192.168.2.4	49840	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jan 09 01:00:00 CET 2018 Tue Oct 22 14:00:00 CEST 2013	Fri Feb 12 13:00:00 CET 2021 Sun Oct 22 14:00:00 CEST 2028	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Nov 26, 2020 06:20:19.132198095 CET	13.224.93.10	443	192.168.2.4	49842	CN=api.demandbase.com, O="Demandbase, Inc.", L=San Francisco, ST=California, C=US, SERIALNUMBER=C3920817, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.2=California, OID.1.3.6.1.4.1.311.60.2.1.3=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Fri Oct 09 23:16:41 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Thu Oct 28 02:17:28 CEST 2021 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Nov 26, 2020 06:20:19.132776022 CET	13.224.93.10	443	192.168.2.4	49843	CN=api.demandbase.com, O="Demandbase, Inc.", L=San Francisco, ST=California, C=US, SERIALNUMBER=C3920817, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.2=California, OID.1.3.6.1.4.1.311.60.2.1.3=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Fri Oct 09 23:16:41 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Thu Oct 28 02:17:28 CEST 2021 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Nov 26, 2020 06:20:19.186523914 CET	52.50.104.129	443	192.168.2.4	49844	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jan 09 01:00:00 CET 2018 Tue Oct 22 14:00:00 CEST 2013	Fri Feb 12 13:00:00 CET 2021 Sun Oct 22 14:00:00 CEST 2028	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Nov 26, 2020 06:20:19.188752890 CET	52.50.104.129	443	192.168.2.4	49845	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jan 09 01:00:00 CET 2018 Tue Oct 22 14:00:00 CEST 2013	Fri Feb 12 13:00:00 CET 2021 Sun Oct 22 14:00:00 CEST 2028	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Nov 26, 2020 06:20:20.120465040 CET	50.16.119.144	443	192.168.2.4	49846	CN=logx.optimizely.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Sep 21 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Oct 21 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 6772 Parent PID: 800

General

Start time:	06:19:06
Start date:	26/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6778a0000
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	Completion	Count	Source Address	Symbol

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: 6816 Parent PID: 6772

General

Start time:	06:19:07
Start date:	26/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6772 CREDAT:17410 /prefetch:2
Imagebase:	0x920000
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

Analysis Process: dllhost.exe PID: 6260 Parent PID: 800

General

Start time:	06:19:24
Start date:	26/11/2020
Path:	C:\Windows\System32\dllhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\DllHost.exe /Processid:{49F171DD-B51A-40D3-9A6C-52D674CC729D}
Imagebase:	0x7ff714000000
File size:	20888 bytes
MD5 hash:	2528137C6745C4EADD87817A1909677E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: 3424 Parent PID: 6260

General

Start time:	06:19:25
Start date:	26/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 7144 Parent PID: 6772

General

Start time:	06:19:37
Start date:	26/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6772 CREDAT:82952 /prefetch:2
Imagebase:	0x920000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly

Code Analysis