ID: 433011
Cookbook: browseurl.jbs
Time: 05:22:53
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

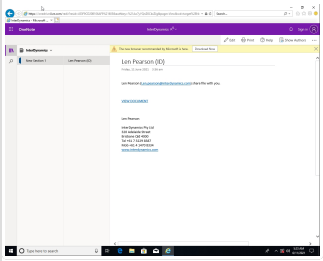
Analysis Report https://1drv.ms:443/o/s!BPlqEAvSnD9F…

Overview

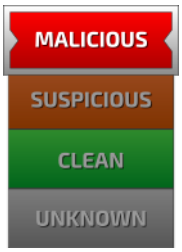
General Information

Sample URL:	http://https://1drv.ms:443/o/s!BPlqEAvSnD9FhF2O8mEJ2egpMWSY?e=fOTayHsLEEiU05h11yffVA&at=9
Analysis ID:	433011
Infos:	

Most interesting Screenshot:



Detection

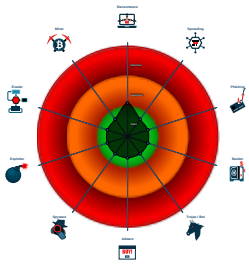


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Antivirus detection for URL or domain

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 5424 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5124 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5424 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 488 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5424 CREDAT:82960 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 1392 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5424 CREDAT:17438 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- dllhost.exe (PID: 3468 cmdline: C:\Windows\system32\DllHost.exe /Processid:{49F171DD-B51A-40D3-9A6C-52D674CC729D} MD5: 2528137C6745C4EADD87817A1909677E)
  - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

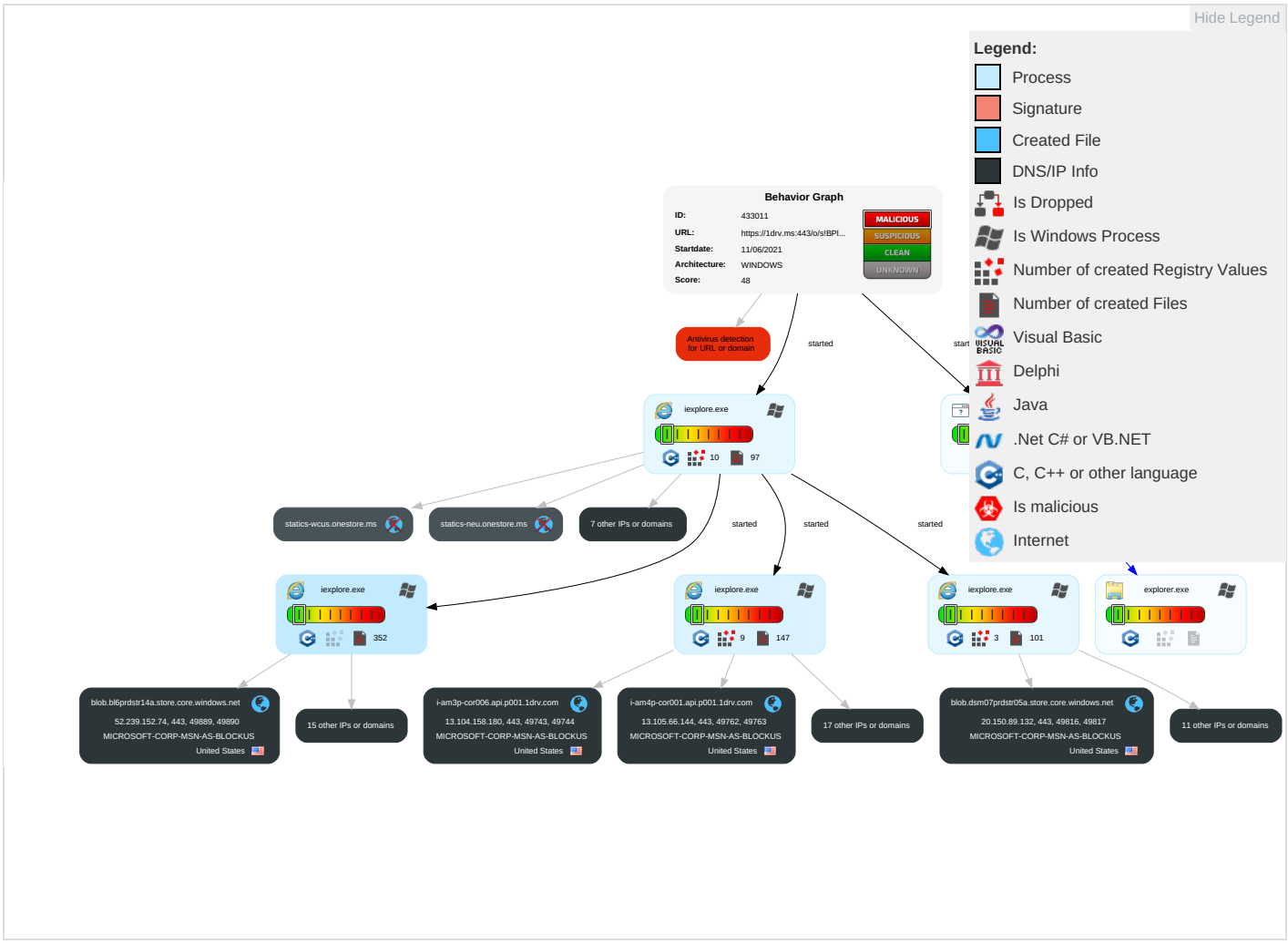
AV Detection:

Antivirus detection for URL or domain

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impac
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 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	Modif Syste Partiti
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	Devic Lockc
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	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	Delet Devic Data

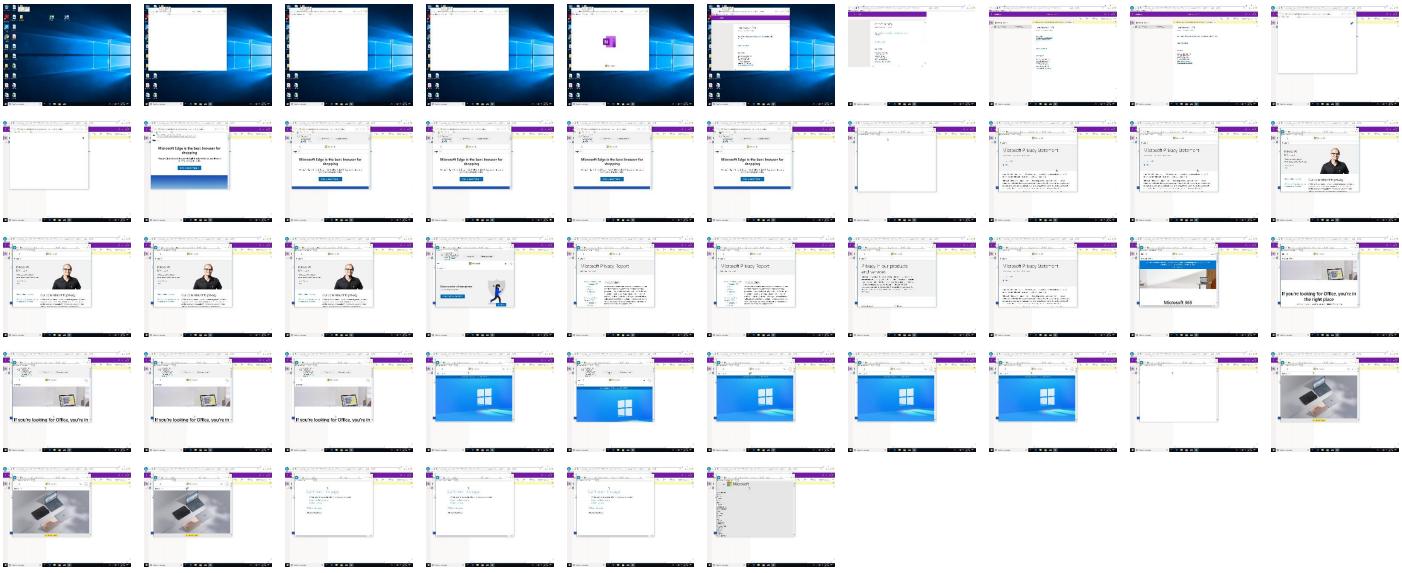
Behavior Graph

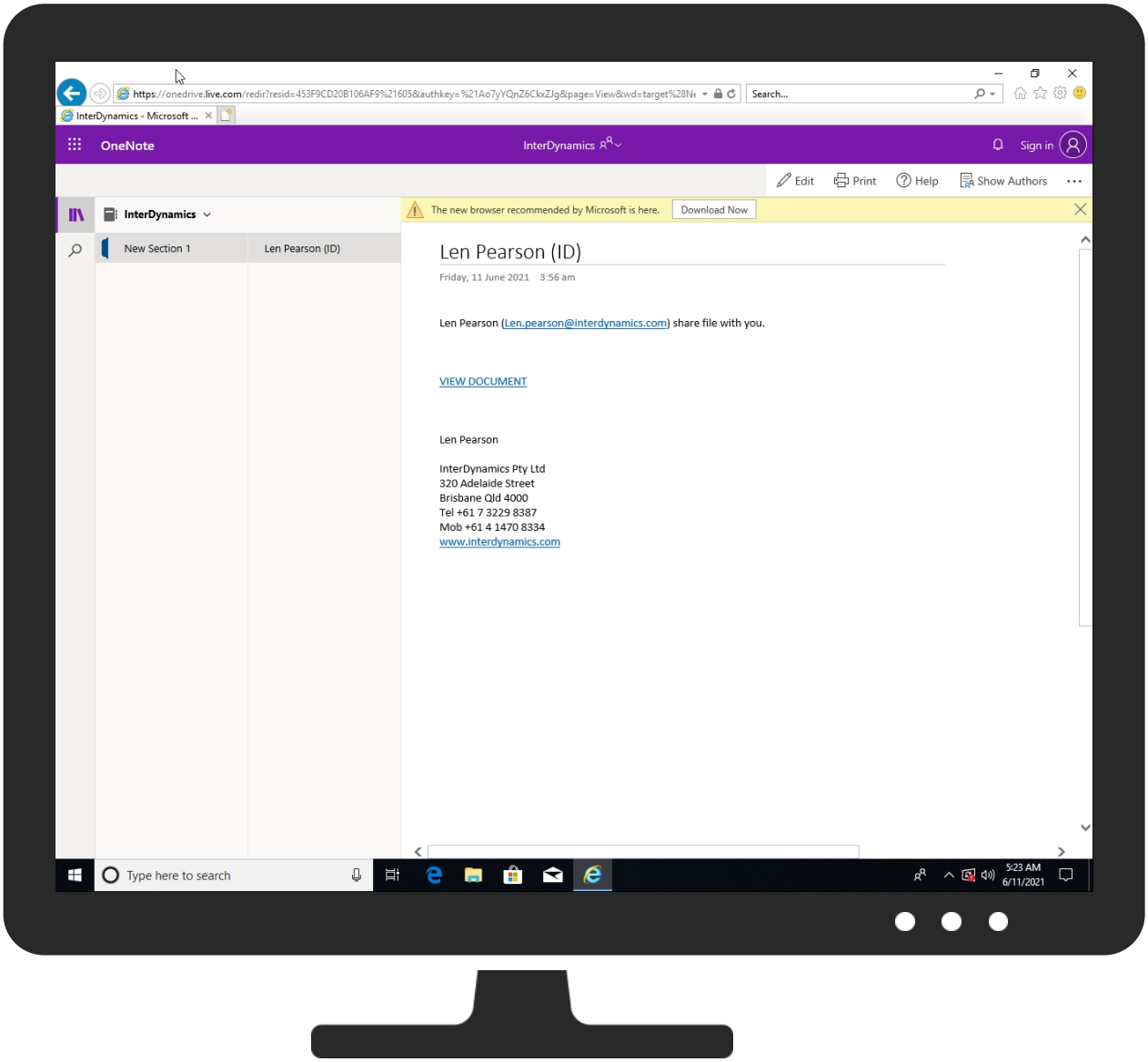


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://1drv.ms:443/o/s!BPlqEAvSnD9FhF2O8mEJ2egpMWSY?e=fOTayHsLEEiU05h11yffVA&at=9	1%	Virustotal		Browse
http://https://1drv.ms:443/o/s!BPlqEAvSnD9FhF2O8mEJ2egpMWSY?e=fOTayHsLEEiU05h11yffVA&at=9	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
sni1gl.wpc.gammacdn.net	0%	Virustotal		Browse
cs1227.wpc.alphacdn.net	0%	Virustotal		Browse
logincdn.msauth.net	1%	Virustotal		Browse
statics-eas.onestore.ms	0%	Virustotal		Browse
assets.onestore.ms	0%	Virustotal		Browse
statics-wcus.onestore.ms	0%	Virustotal		Browse
amcdn.msftauth.net	0%	Virustotal		Browse
consentreceiverfd-prod.azurefd.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://onedrive.live.com/redir?resid=453F9CD20B106AF9%21605&authkey=%21Ao7yYQnZ6CkxZJg&page=View&wd=target%28New%20Section%201.one%7C80ad529f-1552-420d-bb5a-d50e6a192b23%2FLen%20Pearson%20%28ID%5C%29%7Cdbbfcf9d-1ae4-48ed-865e-22967eb5e535%2F%29	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
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://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://w.b	0%	Avira URL Cloud	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://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	

Source	Detection	Scanner	Label	Link
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	URL Reputation	safe	
http://https://privacy.microsoft	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%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	URL Reputation	safe	
http://www.michaelbromley.co.uk/blog/193/a-note-on-touch-pointer-events-in-ie11	0%	URL Reputation	safe	
http://www.michaelbromley.co.uk/blog/193/a-note-on-touch-pointer-events-in-ie11	0%	URL Reputation	safe	
http://www.michaelbromley.co.uk/blog/193/a-note-on-touch-pointer-events-in-ie11	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://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://c1-onenote-15.cdn.offic	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	
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://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%	URL Reputation	safe	
http://www.movable-type.co.uk/dev/keyboardevent-key-values.html	0%	URL Reputation	safe	
http://www.movable-type.co.uk/dev/keyboardevent-key-values.html	0%	URL Reputation	safe	
http://https://mem.gfx.ms	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://mem.gfx.ms	0%	URL Reputation	safe	
http://https://mem.gfx.ms	0%	URL Reputation	safe	
http://search.ipop.co.kr/	0%	URL Reputation	safe	
http://search.ipop.co.kr/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
i-am4p-cor001.api.p001.1drv.com	13.105.66.144	true	false		high
sni1gl.wpc.gammacdn.net	152.199.21.175	true	false	• 0%, Virustotal, Browse	unknown
scontent.xx.fbcdn.net	31.13.92.14	true	false		high
blob.dsm07prdstr05a.store.core.windows.net	20.150.89.132	true	false		high
microsoftwindows.112.2o7.net	13.36.218.177	true	false		high
i-am3p-cor006.api.p001.1drv.com	13.104.158.180	true	false		high
blob.bl6prdstr14a.store.core.windows.net	52.239.152.74	true	false		high
cs1227.wpc.alphacdn.net	192.229.221.185	true	false	• 0%, Virustotal, Browse	unknown
polyfill.io	151.101.65.26	true	false		high
aka.ms	95.101.18.109	true	false		high
1drv.ms	13.107.42.12	true	false		high
js.monitor.azure.com	unknown	unknown	false		high
logincdn.msauth.net	unknown	unknown	false	• 1%, Virustotal, Browse	unknown
statics-eas.onestore.ms	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
messaging.office.com	unknown	unknown	false		high
assets.onestore.ms	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
c.live.com	unknown	unknown	false		high
ajax.aspnetcdn.com	unknown	unknown	false		high
stedgecommercialdev.blob.core.windows.net	unknown	unknown	false		high
statics-wcus.onestore.ms	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
cart.production.store-web.dynamics.com	unknown	unknown	false		high
onedrive.live.com	unknown	unknown	false		high
p.sfx.ms	unknown	unknown	false		high
amcdn.msftauth.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
www.onenote.com	unknown	unknown	false		high
consentreceiverfd-prod.azurefd.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
onenoteonlinesync.onenote.com	unknown	unknown	false		high
assets.adobedtm.com	unknown	unknown	false		high
storage.live.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
skyapi.onedrive.live.com	unknown	unknown	false		high
mem.gfx.ms	unknown	unknown	false		unknown
statics-neu.onestore.ms	unknown	unknown	false		unknown
statics-eus.onestore.ms	unknown	unknown	false		unknown
dc.services.visualstudio.com	unknown	unknown	false		high
amp.azure.net	unknown	unknown	false		high
spoprod-a.akamaihd.net	unknown	unknown	false		high
offertooldataprod.blob.core.windows.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/redir?resid=453F9CD20B106AF9%21605&authkey=%21Ao7yYQnZ6CkxZJg&page=View&wd=target%28New%20Section%201.one%7C80ad529f-1552-420d-bb5a-d50e6a192b23%2FLen%20Pearson%20%28ID%5C%29%7Cdbbfcf9d-1ae4-48ed-865e-22967eb5e535%2F%29	false	• SlashNext: Fake Login Page type: Phishing & Social Engineering	high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.105.66.144	i-am4p-cor001.api.p001.1drv.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
20.150.89.132	blob.dsm07prdstr05a.store.core.windows.net	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
13.107.42.12	1drv.ms	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
192.229.221.185	cs1227.wpc.alphacdn.net	United States		15133	EDGECASTUS	false
152.199.21.175	sni1gl.wpc.gammacdn.net	United States		15133	EDGECASTUS	false
52.239.152.74	blob.bl6prdstr14a.store.core.windows.net	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
13.104.158.180	i-am3p-cor006.api.p001.1drv.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
31.13.92.14	scontent.xx.fbcdn.net	Ireland		32934	FACEBOOKUS	false
95.101.18.109	aka.ms	European Union		16625	AKAMAI-ASUS	false
151.101.65.26	polyfill.io	United States		54113	FASTLYUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433011
Start date:	11.06.2021
Start time:	05:22:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://1drv.ms:443/o/s!BPlqEAvSnD9FhF2O8mEJ2egpMWSY?e=fOTayHsLEEiU05h11yffVA&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:	30
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:	mal48.win@8/508@39/11
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=521839 • Browsing link: https://privacy.microsoft.com/ • Browsing link: https://account.microsoft.com/privacy • Browsing link: https://aka.ms/PrivacyReport • Browsing link: https://privacy.microsoft.com/privacy-in-our-products • Browsing link: https://go.microsoft.com/fwlink/?LinkId=521839 • 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/sale?icid=gm_nav_L0_salepage
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
05:24:00	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\15TFWFSP\account.microsoft[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\15TFWFSP\account.microsoft[1].xml	
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Reputation:	low
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\15TFWFSP\onedrive.live[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Reputation:	low
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\S30Y26QX\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):	798
Entropy (8bit):	5.0123580411258795
Encrypted:	false
SSDEEP:	24:WU1mKm6DPilZU1mKm6DPilZU1mKm6DPilZU1mKm6DPilFqQ/qQ9sDilZU1mKm6DF:LsKPilisKPilisKPilisKPilQilisKPt
MD5:	70B94BFE35BB7C9C8798E66193BB7339
SHA1:	3B329904D3F40BA3DC2FB3DFD4742106EBE1716B
SHA-256:	15FACB97A638D4EBB3F3413C1278DDCB6699BC70F07EDDD30B764F7D9C04283A
SHA-512:	8B9CBA9BF7533767F7535265DB5A57D87F19E1C68AB7539F728259CBDBA2904CB67DE54AB43990172E9C822E2FDAB9D0534E0490C86FF7C6572535D7025C9BE
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="com.adobe.reactor.dataElementCookiesMigrated" value="true" ltime="2964628432" htime="30891708" /></root><root><item nam e="com.adobe.reactor.dataElementCookiesMigrated" value="true" ltime="2964628432" htime="30891708" /></root><root><item name="com.adobe.reactor.dataEle mentCookiesMigrated" value="true" ltime="2964628432" htime="30891708" /></root><root><item name="com.adobe.reactor.dataElementCookiesMigrated" value="true" ltime="2964628432" htime="30891708" /><item name="Fri Jun 11 2021 05:24:16 GMT-0700 (Pacific Daylight Time)" value="Fri Jun 11 2021 05:24:16 GMT-0700 (Pacific Daylight Time)" ltime="2988638432" htime="30891708" /></root><root><item name="com.adobe.reactor.dataElementCookiesMigrated" value="true" ltime="2964628432" htime="30891708" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\TGLKQ5GA\onenote.officeapps.live[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):	87741
Entropy (8bit):	5.074948850365871
Encrypted:	false
SSDEEP:	768:hQSOjZ/OdQSOjZ/ODQSOjZ/ODQSOjZ/ODQSOjZ/OdQSOjZ/OaQSOjZ/OdQSOjZ/3:t
MD5:	02427F9D68A02A87806F319637C6F753
SHA1:	1753DE210081B2133CE3E9D0023753D75B7898CD
SHA-256:	531E9405614BF57444094BBA04D7D592F01B4D6145A0858448CA016AF2544C30
SHA-512:	A270AD66ACEADEC47DDE464680B45EC64EA123F822ACD7869668AC80ED0CE751EA2092EDC2BE3BC5BDBD4D8AD1E0B6216496562FEDA6430FE3C3ACA6AFE 6BE8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\TGLKQ5GA\onenote.officeapps.live[1].xml	
Preview:	<root></root><root><item name="obf-CampaignDefinitions" value="[{"CampaignId":"281ff77f-ec20-4b5b-88dc-674ede3473ee","StartTimeUtc":"2018-09-04T00:00:00Z","EndTimeUtc":"2025-01-01T00:00:00Z","GovernedChannelType":0,"AdditionalDataRequested":["EmailAddress"],"NominationScheme":{"Type":0,"PercentageNumerator":25,"PercentageDenominator":100,"NominationPeriod":{"Type":0,"IntervalSeconds":1296000},"CooldownPeriod":{"Type":0,"IntervalSeconds":7776000},"FallbackSurveyDurationSeconds":120},"SurveyTemplate":{"Type":4,"ActivationEvent":{"Type":1,"Sequence":[{"Type":0,"Activity":"AppUsageNPS","IsAggregate":true,"Count":300},{"Type":0,"Activity":"AppUsageTimeSatisfiedNPS",&

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\Z2REQ4WQ\www.onenote[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	140
Entropy (8bit):	4.972993757702314
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsOHQYMALfVAqJhXIUiREzQnFk6EBM9qSeUSV/K9LKb:JFK1rUFKlMufVAqJhYUhQu6WMleL1zb
MD5:	3CE8D1388E7757384771BE070D219764
SHA1:	B6AC0E99A7191A83084D65D6022FBEFE29C5C2FF
SHA-256:	03D4505BFBCB050A24160CE509F8AB5C8054E71616580F299BDB148700E4541C
SHA-512:	565A8D2C1F29BAEE230A1F2E940C9A0DC584726821A0777489976CACEB77F14EDF983D06990168037B51573F5EA9E9E3D86F7365B28A2F421D3ED16F7EC472F8
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="Office API client" value="c6f670bf-9719-b4cd-b514-10d0168a7e5b" ltime="2813198432" htime="30891708" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{D7B2A239-CAAF-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	99720
Entropy (8bit):	2.333040437313155
Encrypted:	false
SSDEEP:	384:r8975CoS1m4Xdtm6saeduPfYaO5R6HVkhu42C:1Yr
MD5:	214199E81D9C372C086DDB98520A0DCD
SHA1:	0E653032E3C9C5CF71C825AE73CFFA80FCCC97CF
SHA-256:	1EB6574EA7B9A8D9F75A945C57AEED042F540D50CE3CD9EA68EB7CA355EC8B67
SHA-512:	0954E9F13B7EA0FE81FB50DFB46D09047BAF1E55B2790C0B9413EAED8BBFC64C51247FBE334E00A006115F42F53A46E472BDE92CC8FBEF0F660D31178BDFDA97
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\{D7B2A23B-CAAF-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	63148
Entropy (8bit):	3.073029963061523
Encrypted:	false
SSDEEP:	384:rSqccbYQ3P1bXg6EH7mctGLq0Pgp/how7mctGLq0Pgp/hoPFqOT:Rub2Lq0Pg512Lq0Pg5yT
MD5:	2CE28166EB7E5923E64F21A1D8CCC9F0
SHA1:	3A2C073ED798FDA4F37FFA4C83622EA304A8D2A8
SHA-256:	C9006078EDD0D1310F533A9510BF9C14A3208247A43E989C8923F26A80281136
SHA-512:	D6B19FB44045164EF8475EE3AA9D31B7F462D1EEB58CDA7865AB910BAA31BD6980EC2327242EC725B6658C6BB03D61C2E7B5091344C4D12734427E8B6F75895
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\{E40D82AC-CAAF-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E40D82AC-CAAF-11EB-90E4-ECF4BB862DED}.dat	
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5845967511996035
Encrypted:	false
SSDEEP:	48:IwdGcprgGwpalG4pQNGrapbStGQpKOG7HpR5TGIpX2iGApm:rDZoQ36tBSXAJT/FBg
MD5:	52223C275E382D64B2A711AAA40AA386
SHA1:	CFE36E35609A472D81B8F6086BDBB1E0C7E078DC
SHA-256:	88E577F06438850281C3A0BB7EDD74A6FD4062D94360B4FC6B5F7FC2C1575DE3
SHA-512:	E9A3C694EE1F6FC5ABFDCE16BF21F0CBD3FC39CBEC396517CEFC530D06F9ADCC4DF9AB41A50CB39F0C70CB17CA43E5EB521941500820B10193C45A64D3C6 1A8
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\{ECE3944F-CAAF-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	34034
Entropy (8bit):	2.1131792478465745
Encrypted:	false
SSDEEP:	192:rVZWQd63kxjd2pW/hMeAF1/145YD4MTvvtHhvvtHi/Qr:rbjI0NUY/6eI1uCsMQw
MD5:	135C05FAF8F9EB334F2FEDEEDD2F4895
SHA1:	ACB3F91A148779852F8E37D293A0F8022D147690
SHA-256:	9C732F40A37629B571AD8239FC3A4D1088FCB8F4E3B9AEDB6EE398609F35934F
SHA-512:	E99C288CC253132047E780FA7C9B2F408D6987D0ADD0B8E469DF153F7B91D37496B18B6F0D7307FDF084CCEE065E4804AB77C8F7A9AC643CB78987D299B82A1
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\{ECE39450-CAAF-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5855266851303231
Encrypted:	false
SSDEEP:	48:IwNKGcprHxGwpa1KG4pQ7YGrapbSZGQpKrG7HpRETGIpX2pGApm:rNuZHrQ1q67mBSzAqTAF8g
MD5:	94ADD843FC8BBFF60F75EFDAC14FF72D
SHA1:	B7FDF5E9A44CCA64D36BC35272FB2EB0FD1D7191
SHA-256:	76D2EB4C7FE68621C92D375088012A061073C3E543CBB564E182EAFD0D03D112
SHA-512:	BC4C6545B685926FA774053B023ABCCA3D4C013D3FC4EF4187EA19208564BFF98B46793385C5038D5FCA74E077F9B7AB0398D5F2DC428D6C402C5E13BC1B235
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\{F639C9D3-CAAF-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	239784
Entropy (8bit):	2.875571215557668
Encrypted:	false
SSDEEP:	1536:17I0DMk5gORnkdUgOVnkPdRnMsMvMsMbMsM0VMsMvMsMbMsMJJh:ZMk5pRnkdUpVnkPdRHMfM7M0FMfM7MXh
MD5:	DE50279C077B56FE3013524963944D6E

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F639C9D3-CAAF-11EB-90E4-ECF4BB862DED}.dat	
SHA1:	6AB62A6A387926C3627F8105D952BD34D26BE565
SHA-256:	65A5531CDC0B797871949B8AAB3B1DC95A90DB09F8D2D3102A64CDCF7D11799E
SHA-512:	0E0C030399BC2366B782EA4F08ED2D1DCE257115620623322733 7D72F051C7EE9E94F7EF0D8773E11E8A913FC34123DD3071CD044B648333610CA5CA7CDE9D7
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\{FF8CF6E6-CAAF-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5663293737082422
Encrypted:	false
SSDEEP:	48:IwPGcprCGwpaXG4pQDGrapbSjGQpKtG7HpRJTGIpG:rFZqQZ6nBSdAMTvA
MD5:	B501584425593140B9D078503B32FE98
SHA1:	F21AFFBB3373CB80A54493862806284B3E1DE29E
SHA-256:	199E15FB811ED33543ED8B60E471A791491C90BAB3E46CBB3DEBE61C960BDF4E
SHA-512:	C1E23A9BB5B1105F5194F6CF9BCA1CB87E0D2E3E83ABB66760B4461BD1F7574EE45C12B8F57B0C9EFAA011A631B640059E9E2F884B3B2E85A73DB4D784BFFFC9
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):	5.030782504575926
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE3X4InWimI002EtM3MHdNMNxOE3X4InWimI00ObVbkEtMb:2d6NxO8VSZHKd6NxO8VSZ76b
MD5:	26D26633A4192AAC1698F0A766E7B2BC
SHA1:	A2178AC9E6178B04423151C22F5EA7A0A69EB704
SHA-256:	E2A1AA1E99F9FD5CDEC857E10D83623B9D485431379A4F51301B5B1476D14207
SHA-512:	963E357B2DE0D4DCCC0D712A249B889C0F90AED62AF7D40F6D4A92CFD0042A1ED8B922F69EA0189546691A75DEA3113229D2F70AA1C9D33BFAE69FE0FE3900C8
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xb1ac0d3f,0x01d75ebc</date><accdate>0xb1ac0d3f,0x01d75ebc</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>0xb1ac0d3f,0x01d75ebc</date><accdate>0xb1ac0d3f,0x01d75ebc</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):	5.069446739226235
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kYCXlnWimI002EtM3MHdNMNxe2kYCXlnWimI00Obkak6EtMb:2d6Nxr0VSZHKd6Nxr0VSZ7Aa7b
MD5:	D587356602E78BC062510C71FDF41680
SHA1:	3E660FBDED8FDBD57A6ABEEE02E44CB33D5312CA
SHA-256:	6F9AD4237C7F5A91EB6111332F0261DE0477C3DA71215C9DC4B40F70FB836188
SHA-512:	4FCD8D0D01DCDD61F96E4FFE82D069D8A32ED1915CE387AF814D67AF1E658C09CA3A082E11D24DF2E777B37988F14C20C9EF344F69DC29721D20820246F960I
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xb1a41dfa,0x01d75ebc</date><accdate>0xb1a41dfa,0x01d75ebc</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>0xb1a41dfa,0x01d75ebc</date><accdate>0xb1a41dfa,0x01d75ebc</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):	5.080990358054866
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLhgFWgunWimI002EtM3MHdNMNxvLhgFWgunWimI00ObmZEtMb:2d6NxvtgFWguSZHKd6NxvtgFWguSZ7mb
MD5:	D95D21790B85ED639FA313C209B95B4E
SHA1:	0CB87070EB8FF2CF0F47049F3F011103B31D96B9
SHA-256:	DC026E2F241931AF283743D7DBAA06565131EA1BE73229C1958F3530675B32AD
SHA-512:	F050896DF5448D1C9A43F28CDAB3B6CFEB48AC60D4A52F821B760E7C9E0A1B5B1F650B7A689603CD13E5EC8D1512FDCDF386B79FDE07F11FE36AB7E195E4E54B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xb1b36030,0x01d75ebc</date><accdate>0xb1b36030,0x01d75ebc</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>0xb1b36030,0x01d75ebc</date><accdate>0xb1b36030,0x01d75ebc</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):	5.045657436852529
Encrypted:	false
SSDEEP:	12:TMHdNMNxi3X4InWimI002EtM3MHdNMNxi3X4InWimI00Obd5EtMb:2d6NxeVSZHKd6NxeVSZ7Jjb
MD5:	EF83C278B92D926EE0B8AF5D1637F93A
SHA1:	5E1AEA3E12761BE31BFFF7B55C463E1B25F1E6D7
SHA-256:	EC3244F6513C7180A7A49AF16B0EC1C67B684ADDE4F1791264335F6A0D8CB621
SHA-512:	95F8A154FE33470ED7FC3890D89DF31F2525BCC715CF094CD8044B42678660901730FD5094514EE67EF5847D3FECD02EBADBC85C5EC17F0A3B2651EE7FA014A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xb1ac0d3f,0x01d75ebc</date><accdate>0xb1ac0d3f,0x01d75ebc</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>0xb1ac0d3f,0x01d75ebc</date><accdate>0xb1ac0d3f,0x01d75ebc</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):	5.087731053065231
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwhgFWgunWimI002EtM3MHdNMNxhGwhgFWgunWimI00Ob8K075EtMb:2d6NxQ8gFWguSZHKd6NxQ8gFWguSZ7YV
MD5:	841C0CBE3B5BBB653096CCE65FD783C2
SHA1:	5C44649537CEEEFA718C844F75CCDA3CF6F4D443
SHA-256:	02C41DFB6CE9F203175A389517FDC8B069791DF45466B0731E420BECF3D60B36
SHA-512:	FEE7B24D9ED2FE365864188425B9FE86CF738C15B1A84462F77E45CF0FB5FF1C50600C75C32D91D3C9D7095C67FEB24CF92CD427D383A0C4E06F12F7CEFF4F0F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xb1b36030,0x01d75ebc</date><accdate>0xb1b36030,0x01d75ebc</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>0xb1b36030,0x01d75ebc</date><accdate>0xb1b36030,0x01d75ebc</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-6757900\msapplication.xml	

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):	5.03122909378017
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n3X4InWimI002EtM3MHdNMNx0n3X4InWimI00ObxEtMb:2d6Nx0nVSZHKd6Nx0nVSZ7nb
MD5:	9A8853914F28F311CF4F09F5643D8DD8
SHA1:	760090B705E8A1FE88BB0D97C9A9CDC0FED79FEC
SHA-256:	544615252606120ADB5126A0FCBB2CBC76CF619DB598319C0A5BC72E06C314BC
SHA-512:	606032E9AF04E1099E563ABC814261FF317A373CD52482EB077CDA21A361D64950AD4297363ABE44EB513FA40DBBC2D48DC9D22B11B0CB403593B671E53D942
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xb1ac0d3f,0x01d75ebc</date><accdate>0xb1ac0d3f,0x01d75ebc</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>0xb1ac0d3f,0x01d75ebc</date><accdate>0xb1ac0d3f,0x01d75ebc</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):	5.0712062058466225
Encrypted:	false
SSDEEP:	12:TMHdNMNxx3X4InWimI002EtM3MHdNMNxx3X4InWimI00Ob6Kq5EtMb:2d6NxdVSZHKd6NxdVSZ7ob
MD5:	E2980E0C7557A5BA271AB3F8BAE5B684
SHA1:	E13B4EE8A35032D05B4474C98C8BF2C8280F994B
SHA-256:	467FAF6248D80D51200F400066ED25E2F97DB1284D907F3546E2E3A47925BAAD
SHA-512:	B9A6B7E291AEA182E88E01A57F4309DEACBD56D0F1CC369994F7A437DB5B142A681CB1E509287EBE7E20F3703024F1D0FBB02BC51A0497AECAE83D136A5C7005
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xb1ac0d3f,0x01d75ebc</date><accdate>0xb1ac0d3f,0x01d75ebc</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>0xb1ac0d3f,0x01d75ebc</date><accdate>0xb1ac0d3f,0x01d75ebc</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
Entropy (8bit):	5.060669154541902
Encrypted:	false
SSDEEP:	12:TMHdNMNxcYCXlnWimI002EtM3MHdNMNxcYCXlnWimI00ObVEtMb:2d6NxsVSZHKd6NxsVSZ7Db
MD5:	CCA8EEA9AFAA22816BEAF457F85ED8D4
SHA1:	6A3EF6902497BAD2ADC3549C85ADF100577122AC
SHA-256:	DB641CFC148978501222EF0D85DBBF696C98ED40F2CAA7E1F3C061108509B3FD
SHA-512:	FC79488D0FBFA6A927FF9C68B5444DE20998C62958C6C9EA92C042C97877C9DC06A6A7468DBE62E5A17E829490D7C2A674206C760C1D20E493A49037327A48A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xb1a41dfa,0x01d75ebc</date><accdate>0xb1a41dfa,0x01d75ebc</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>0xb1a41dfa,0x01d75ebc</date><accdate>0xb1a41dfa,0x01d75ebc</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):	5.049772370537285
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnYCXlnWimI002EtM3MHdNMNxfnYCXlnWimI00Obe5EtMb:2d6NxvVSZHKd6NxvVSZ7ijb
MD5:	90EC38BCB9AEDBD0359E72E06A8F7321
SHA1:	53317D5C04DF8A85DAE933AE263145232E46A48E
SHA-256:	5C799DEC1C452EEF620700C7DF8AA5A496C388885E352AFE641631007842F657
SHA-512:	B4EFB3301276A1D977557E1C7AE646BF12C3059E0727D6DE02A292E526F70336A23F68634A3520A9C3F4F7D4A48A21DBB33CF9BD99BC78DC758AFB08C309D45
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xb1a41dfa,0x01d75ebc</date><accdate>0xb1a41dfa,0x01d75ebc</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>0xb1a41dfa,0x01d75ebc</date><accdate>0xb1a41dfa,0x01d75ebc</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\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	53748
Entropy (8bit):	3.041079220968083
Encrypted:	false
SSDEEP:	48:bAlA0A0AGgyyyyyyyyyyyyyuA0DA9QQQQQA6H6K6C6tgyyyyyyyyyyyyyT6DW6GQ:qQQQQQoQQQQQ4QQQQQt
MD5:	C2F7464F440CBE5ED1C919EE2622D2FE
SHA1:	0D288DC77FDEE0AA437E8FA1987E806D5C343ABB
SHA-256:	F5DAB319EF45BF86E3F0E8B969D71123CCB1E5A1F601258F1B4B9268D51AF019
SHA-512:	35AC86CA4DD8ADC03A11363C9B7CA9C91F79D042DF61D2F59728C14663745FE0848FD2458783D13A488D648F7D9EB04C8DCA641BFA9AE8D0869B92EEF4AE59B
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...'' ...3333333333333333333333333333333'' ...3333333333333333333333333333333'' ...333333333333333333333333333333333'' ...3333333333333333333333333333333'' ...3333333333333333333333333333333'' ...3333333333333333333333333333333'' ...3333333333333333333333333333333'' ...3333333333333333333333333333333'' ...3333333333333333333333333333333'' ...3333333333333333333333333333333'' ...3333333333333333333333333333333''''''''''''''''''''''''''''''''

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1-WebBrowsing-01[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 370, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	31965
Entropy (8bit):	7.9519959589170695
Encrypted:	false
SSDEEP:	768:G2+elgXGKSKgipe/3Nj2X8f2BS+oiJRKFYcWA:G2+esGKQiOcX2aSWc
MD5:	255DD67FA877795019867502F4095E85
SHA1:	0B3E8F077AA858C6F3613D1607CDF7BA699E6FE5
SHA-256:	BB88C60C19E587AD0793648DE59E089D35F424ECF0BFF9FD28CF33D16ED1A767
SHA-512:	96F6569C42781418C23B59F7209CF095BA5D54C47572B33B0F04DEA94DA1CD6882A6AF94241B09164CF518D66CC1D7739C834801CD62EBB252E1310C7186C818
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1-WebBrowsing-01.png?version=280edfb3-3250-3e5d-5f4f-35711788a8a7
Preview:	.PNG........IHDR... ...r.......).....pHYs.........8''.@...$zTXtCreator....sL.OJUpL+I-RpMKKM.)..Az..jz.... .IDATx...y.\.] .s.^U].U....e.%...o.......3d..0.....yC^`x.......d.$C..Y..qb..^c.l.-Kj. .}..k...3.\..j.^..R..~....{...............*..x.^..eg.....X...N..z...G...... ......0..X.....&........d.`........,......A......`2.......L......... ......0..X.....&........d.`........,......A......`2.......L......... ......0..X.....& ....p...x.g..cl..)...B...SJM9,...`#...za.%I.8.?3.c...I5.,UUu]7.,..... ...1.x<,...,..0..q...,.B.z:....H .....|...<.1.q,.*...*L....p.(r.k...<o.IEQ.$.b/....2.`...X.Q..y<.|.......0EX....c#..,.....'..BI... .......u........a.I...,.c...p...J..0. p.W.q.b,... ..........V.`YV....W.y^.4h......J.f...<..zK8.Bo.+.{......J.~.up..E''..eMo%.......,.c.F...+.Z...[....... .r=A.J{fp..e............v..R.c.6.....6gk.K../.......c... ._....B..b[6.c4P._W..p..C.w"J...k..u...`.........u.....@..I...Y..n..<!DUUUU...|+.KF..Q................l.....\.......(dA7.[!.)B.0R..g..]m.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1083_Panel09_4Up_LearningDisability[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, 235x132, frames 3
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1083_Panel09_4Up_LearningDisability[1].jpg	
Size (bytes):	11227
Entropy (8bit):	7.94946638756173
Encrypted:	false
SSDEEP:	192:fJm6HBdLK9j5I+8wvBmvpULXIJ0q7AwKvxkpDEcyxqvrYyrrUOqyXLuhATfNeuky:fV/W5I+xvBipULXO0mAXvQy4vkyrrUOJ
MD5:	6DA48FF63C924D1929B6C302C1E663A9
SHA1:	D36CA1A3C3049F7EAF004E9B93F9A6B9EB20E9BB
SHA-256:	CCA3BB40DD14462E7AF3CBD99FEE6723E6549DBCF4465CB163734970760CFA56
SHA-512:	A0AB9C0920C95D4C62FBBEA76FCFC59F3F3CBEE2F406160C0163D30086A22584AEBDBAE9DEAB198EB24A7F86FE86DCCA03F8EEC3E4DCFD58949E7C893A9AEC7C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1083_Panel09_4Up_LearningDisability.jpg?version=a9d3a896-a9b5-0ae3-15e9-ab5e099870de
Preview:	......JFIF..... ... ..v.}.T.6....0..d&.XUB(\.r.. 1..P.ZD|7.8..Rb..Q.,. .*T..k.uI.v.iBf..GSM...%.A. .*T.b..rT...ux..\.Di.@.P.p.....,..6 X.r....X.82.ks.*Z.... K.,\.Uu...fh..~K...5.i...0.,\.b.....z.e ..P..>....a..`...w...G....c..i..Cm=....`.\.sW.(.,...c...(m.1....`..[.dmj.~.i..=.....P...;D...O8-h .a...D0.^..... ...Dv.iK.vb..6....(...6w5K....\..e.1..%z9E..V"..o...9O>.5...._..,p.q.W....^.W....c..Kog...=...Ik.P+..m.km..C..Tn..1....~.s^.t....NF....(a.....5....i_C.....f'X.<n.N.+...`.Nt...4.....vDU.BI..w<z..v...V.!.....S5v.....(.S...lL.N.D. .(UE.NJ..J..sz.f..I..."...p...J.:....".....t.&`..."I..B..s..Fj.e=e.H$P.,.i.[). .t.I..,.&.....d.I Y.....R$.:....C._H.M....JB..H..F.J.ne=.|...^.H.r\q...t.=[.....*..6e.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1083_Panel11_4Up_Organize[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, 235x132, frames 3
Category:	downloaded
Size (bytes):	12381
Entropy (8bit):	7.9331757868055455
Encrypted:	false
SSDEEP:	384:fpJ38JtlyT5Hj7CVYR1MddbU7a4nxkfAj:f3yH5D2+fEAJX
MD5:	A7851FBC67836BB6B0BF057FA9262C50
SHA1:	6B78EA15A8797D56641EF01939FE49CAB5704C61
SHA-256:	45784D78F998F0E85EE1EA794B47358926AFCF5BC9595E676CFA81D710CB997A
SHA-512:	E4896165F6AE452F93CEF7C986681F210C9379E84BA73616BD9440E01E57917B7F7454E5F263F6037C4478A49EB6358D2439C5A2A13E62194F9ADD4EF2D4B03A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1083_Panel11_4Up_Organize.jpg?version=3896d283-8ede-133a-b693-d6074900172f
Preview:	......JFIF.....}J.=....'3....D...i...j.a..p.w.., .D=....@AI.,Ws%[u..Ty82D.kh\..tp.....D..|2..I...5g..a.....i..z.o.q1.YL..p...B..!.Zc.(.w>Ce..S.N=<.....O.T.+l{G....RH...n{w.~U..O...V...%..?..r..$:....T.>..\.y..5.....K.?..'....k..{.....kQ .._%...?...XF...'.}l..p.x..4...r....&c{.%a5...P"...N..=;.c.....K...^.f[..J9!..:...F?+`.r...afmK.\|mG,k;...!u. >9..G5y..*/"...,.....X..%N.Q...S.....{e.yXr.<..hz\|H....8._..... .....oBS...u 0....._... .z.$L&..D...7.`.....um2..U.H..D.bc@.rh...Q.G....u,....."H.G..u-...=f\.$l.wN.mx.6....h4j...;sB.p.\8.w.:.LG....]1j..X..*m..q_...G...s_..^.....(c.g...R}.>D. @.;..Vl..\|..]...$....;u..:.tnjJ&&..1..&...=.w...a11.....On...@....=Ye..ws..P..8..(.L.6.."Lk.t.....`

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1083_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, 1083x400, frames 3
Category:	downloaded
Size (bytes):	20032
Entropy (8bit):	7.502955298274388
Encrypted:	false
SSDEEP:	384:wlDY+ngX4zrTb52TyqydrTDZnaygTjwpykpw4blytWOUcqP2:wJRnhsyqsjZnayEkp7bUtWOUcqP2
MD5:	60B33E181A383283E6E96A9F40BF4045
SHA1:	7BF1BE1FE9AE44A1F94BFF9DA0C53D75715328C6
SHA-256:	AD6C804544415CFE232BC74D83F39989F4D2D4EB187A6ACB07FD6ECDE2493A33
SHA-512:	11EAA578B152228D4C2611106F8D34CD59556C0614DDED6418EFC8714AC39C88A7EDDDA61DC751ADF5FA979F4D30B8353540992960249AA9E927F8E94452C0D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1083_Panel15_Mosaic_Item1_Gray.jpg?version=38f7b9fc-53ec-4997-cd72-7fedd363404d
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:E848B4315CB911EA88EEDBD181122FD0" xmpMM:InstanceID="xmp.iid:E848B4305CB911EA88EEDBD181122FD0" 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\0W10PBUV\1083_Panel15_Mosaic_Item2_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, 542x400, frames 3
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1083_Panel15_Mosaic_Item2_Apps[1].jpg	
Size (bytes):	38181
Entropy (8bit):	7.972806505845131
Encrypted:	false
SSDEEP:	768:Wjas8epJSJt/0nxiEVOjBozNJnjYWRXV8PkPWU9N28qucsyf7nGTdVDJBry6bC:WjBXvSJS0EVOjizN1picPWiNVTtUnmVs
MD5:	E63D4D61B5B3A18F5CD4E4FA271056C0
SHA1:	8FEC124C254725B682BE9B027F565800B9CEC9B5
SHA-256:	EA569F8F6B9C3E0172EAB722CC6021ED001386DC7AD3839EC2E4E90138774F22
SHA-512:	D06906041F5D36C17C062E930551A3C02B34CE5024D6137E18B82EC5CF3226093ECF861F3C1FFB1E82C96BFBB8F1736EF44E9E4623B213427898A36F0784290A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1083_Panel15_Mosaic_Item2_Apps.jpg?version=9263244a-955d-7b74-89b4-35f246bbd01a
Preview:	......JFIF.....i1<....Hy...)b.]}.).V...1&.Zx#.i. .kW.Zv..b...i....<<s.^....)HC0.T.,;.e..Z.88itx.7.\w.. Y'.A.M...ab..K9.Z.....t...#2.&....Th13..Hl@.HlMde.4o].q.0....5.v3..&$...P ...hm.x..y..m.bi...Y.Ca.M.....Yj...$..$3!4. m..Rcg.i..r.....&j.VKK.`1..$..d4."...L.x...1.....Zg..x..X..c.....1.G....-....M.,L.S..i..H..z.Z|^E.....&.h.....x.GX.;....hz...).K}.v..|....I..*rS.F..F..h..0.`d.a."..#.;..We...cBi.f.]:Fo~Q.3LD..x @3.....U..T..S..o.....k$...&..)=S.-...9,D0bli...l4..o...a1.H....l.C.....uJwO.....`....v[ntz...~x.&3#+...;"..U....S-m.`.FBx..1...e.....SL!>_...-.5 .....vBy...c.)b.p6.w}.a.vC.G.....d... ..._.n\....z....L2.....}.Z.....`}H.....!.Hid.x....Q/.4.._.x.68.....5.>g.k.@BNM..*...!.Y.,~..G_...&.t._._:.cA.n.y...{-.G..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1083_Panel24_3Up_Footer_Surface[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, 321x180, frames 3
Category:	downloaded
Size (bytes):	18894
Entropy (8bit):	7.974846897993118
Encrypted:	false
SSDEEP:	384:fS+FzrzE1nFNwigLKvTDce4ItWSDgbesh9eEPAQIt214ttB5lVVbM0bW/318:LExFNQgAe4II9Cs9PAHx6Z2
MD5:	D34A4DB8A6BC6C261819816DD9F0E6B8
SHA1:	EB4B0CB144768071E72DDADCAFA2E567F28ADC02
SHA-256:	43D1D7F12F25D15182097B756EB63C9452B338387907C4D18BE6CF158E8EF8F9
SHA-512:	1E1303A8B8BABB9F46CDA09BA3CF2A8A116EA297EED8C0AEF3399387F406D7A041830D216300BBB43980AEB96C5B13EE6C6A087EDADB123A11CE61B3FCE0C 011
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1083_Panel24_3Up_Footer_Surface.jpg?version=d7a44b09-8bdf-5e60-ad90-b6765c8eb98d
Preview:	......JFIF.....A.....*,r....M.....P'{.{..E..kTG.... ....J|.K.j5."tg$o9Q..,....#b....>..yY..>o..}`.I.:K...^...ZU.6U.D.z.ET..\....Ny..3[.....H.9..\;K9.M...6{...:Yk:E./R..Dy.;kW..PK.b...B...>Z....n...wDJ>....N...JyO+!.cQEe.9zI...=.. .O./...u...dy'...i.'.....{.u...'85...o...wM.t.#+.Q.h]...2..)R.I0.....a.SC.,.....5...}oS.DS.}.....Fk.u..\....n...e.(....^..[...y...`.0.d.O.....,b..=Eu..6(.:....?..0C...Z....Yg.=...=")*...U.I.}..}.....3 .L.....D.....v&G.3..c...tB....!.a..$.^...[/....T.>^^.,...;..E...D..1..d..@...iK...Z..k.G.[..^.*...:....!....`..&M..".....=i[...+..L..5".F..Ge.....gLRRS._...y..g)z...ieMl.T..+U.1..`....U....Ka....r.. ..,...K.....,[....4g..Q.4\...p&$..c^....=....aH.iZ..V)..R...`...YD..8T..b..Lw'W...(..)#..a..-V#..iI)+LN[69

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\17-f90ef1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	136025
Entropy (8bit):	5.225099741417248
Encrypted:	false
SSDEEP:	3072:1f/HuFzpxJIS20i9d1EwgXA95KrtDCE4t:1f/HuXIZRvt
MD5:	942DAE57D4E1D63BA153D2AD9F3D2FAC
SHA1:	0C6F2E447F1FBD839A71FBECEC05DA63D917AEF4
SHA-256:	C136857D2449FB47E6C43792D4B296DFF96F4BA5AAB06F899BF525B17DD4D4BC
SHA-512:	8A079120C12FA817AB8DB2430EB79FFC01AD7627DD432D97C556AF2F3448CD15BB6CA0B91C22815304492AC7385BDDC05748C16961E9B6F44CA8C29E19E680A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-eus-prod/shell/_scrf/js/themes=default/54-af9f9f/c0-247156/de-099401/e1-a50eee/e7-954872/d8-97d509/f0-251fe2/46-be1318/77-04a268/11-240c7b/63-077520/a4-34de62/bb-d7480b/db-bc0148/dc-7e9864/6d-c07ea1/9d-b58f60/f6-aa5278/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/79-499886/7e-cda2d3/69-13871c/6a-234a32/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/17-f90ef1?ver=2.0&_cf=20210415&iife=1
Preview:	(function(){/**. * @license almond 0.3.3 Copyright jQuery Foundation and other contributors.. * Released under MIT license, http://github.com/requirejs/almond/LICENSE. */ .var requirejs,require,define,__extends;(function(n){function r(n,t){return w.call(n,t)}function s(n,t){var o,s,f,e,h,p,c,b,r,l,w,k,u=t&&t.split("/"),a=i.map,y=a&&a["*"]||{};if(n){ for(n=n.split("/"),h=n.length-1,i.nodeIdCompat&&v.test(n[h])&&(n[h]=n[h].replace(v,"")),n[0].charAt(0)==="."&&u&&(k=u.slice(0,u.length-1),n=k.concat(n)),r=0;r<n.length;r+ +)if(w=n[r],w==="."")n.splice(r,1),r-=1;else if(w===".."){if(r===0||r===1&&n[2]===".."||n[r-1]==="..")continue;else r>0&&(n.splice(r-1,2),r-=2);n=n.join("/")}if((u||y)&&a){ for(o=n.split("/"),r=o.length;r>0;r-=1){if(s=o.slice(0,r).join("/"),u)for(l=u.length;l>0;l-=1)if(f=a[u.slice(0,l).join("/")],f&&(f=f[s],f)){e=f;p=r;break}if(e)break;!c&&y&&y[s]&&(c =y[s],b=r)}!e&&c&&(e=c,p=b);e&&(o.splice(0,p,e),n=o.join("/"))}return n}function y(t,i){return function(){var r=b.call(arguments,0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\17-f90ef1[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\17-f90ef1[2].js	
Category:	downloaded
Size (bytes):	136025
Entropy (8bit):	5.225099741417248
Encrypted:	false
SSDEEP:	3072:1f/HuFzpxJIS20i9d1EwgXA95KrtDCE4t:1f/HuXIZRvt
MD5:	942DAE57D4E1D63BA153D2AD9F3D2FAC
SHA1:	0C6F2E447F1FBD839A71FBECEC05DA63D917AEF4
SHA-256:	C136857D2449FB47E6C43792D4B296DFF96F4BA5AAB06F899BF525B17DD4D4BC
SHA-512:	8A079120C12FA817AB8DB2430EB79FFC01AD7627DD432D97C556AF2F3448CD15BB6CA0B91C22815304492AC7385BDDC05748C16961E9B6F44CA8C29E19E680A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-wcus-prod/shell/_scrf/js/themes=default/54-af9f9f/c0-247156/de-099401/e1-a50eee/e7-954872/d8-97d509/f0-251fe2/46-be1318/77-04a268/11-240c7b/63-077520/a4-34de62/bb-d7480b/db-bc0148/dc-7e9864/6d-c07ea1/9d-b58f60/f6-aa5278/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/79-499886/7e-cda2d3/69-13871c/6a-234a32/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/17-f90ef1?ver=2.0&_cf=20210415&iife=1
Preview:	(function(){/**. * @license almond 0.3.3 Copyright jQuery Foundation and other contributors.. * Released under MIT license, http://github.com/requirejs/almond/LICENSE. */ .var requirejs,require,define,__extends;(function(n){function r(n,t){return w.call(n,t)}function s(n,t){var o,s,f,e,h,p,c,b,r,l,w,k,u=t&&t.split("/"),a=i.map,y=a&&a["*"]||{};if(n){ for(n=n.split("/"),h=n.length-1,i.nodeIdCompat&&v.test(n[h])&&(n[h]=n[h].replace(v,"")),n[0].charAt(0)==="."&&u&&(k=u.slice(0,u.length-1),n=k.concat(n)),r=0;r<n.length;r++)if(w=n[r],w===".")n.splice(r,1),r=1;else if(w===".."){if(r===0||r===1&&n[2]===".."||n[r-1]===".")continue;else r>0&&(n.splice(r-1,2),r=2);n=n.join("/")}if((u||y)&&a){ for(o=n.split("/"),r=o.length;r>0;r=1){if(s=o.slice(0,r).join("/"),u)for(l=u.length;l>0;l-=1)if(f=a[u.slice(0,l).join("/")],f&&(f=f[s],f)){e=f;p=r;break}if(e)break;!c&&y&&y[s]&&(c =y[s],b=r)}!e&&c&&(e=c,p=b);e&&(o.splice(0,p,e),n=o.join("/"))}return n}function y(t,i){return function(){var r=b.call(arguments,0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_Panel03_Banner_StayonTrack[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, 319x175, frames 3
Category:	downloaded
Size (bytes):	22127
Entropy (8bit):	7.97303135615474
Encrypted:	false
SSDEEP:	384:fe3fEE89k9fcFMAPYvbHl1QoAU9fqvwiszc67KQAXnZ4X7lBe39ja:ofEE899l3QrU9OwiGqnZwBBepa
MD5:	8DE360BD280335CA4EB199888252B72F
SHA1:	D76A8ADBE21D2E3C6B190CFA03A6671687C664AB
SHA-256:	6657B4E1C66B69E166F70BFBE9BF59F9A6E7D2764C8B3259AD7D363AA0943C75
SHA-512:	4AECEC0CD0D4D00BF00A4278314D828DAD3315B2B7C6BE76D2311E8D4DFA74352EC2FD4D11763F914990A67403167C1BCB16D8296AD7E4A7FCBC585E10881C B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel03_Banner_StayonTrack.jpg?version=b9ff2aa4-ba31-cad7-3920-ed5467501d7b
Preview:	......JFIF.....?.....I....M...Y8.f.'.:P.....U...3..... ...,..rf..)...Y8....0e.WA...uJ{.Y....S%....#._BP6..nc~|..%...nN.gE.?.k=../u.....S...^.....ei.m.x'.....q...:...:...H.rn.t/.v_k...t...8...G:.E..!.V.r.4A!\.4/...[fb..@I...k.c<.1.....L.}Q....i.../... [k-](c..h.!.0C1.....f.M5.t.C..qYR;f.{c....gt.....t]...c4...8.ik^.....xq.P.#.3:Q..>....yg@.....@sP..;..[COT....1..}.B..e..gDp...,..4..~.%(..%.ms....<1.}.j..T...O..E.e.F.l.e.@'.a5.%... ....oz>...#...g..\.o}.....c.....M.z#..E....w[;.@..''l.n..v..Pd.....?.[.Pj.9..#.z....J..+..%.....|....M....{.H...E...2&lriF...I.Be>...#...5.-9;.J<!y.:Ud...7.....x..\...H..@.Cq....X.....ak&. &t..1.k..}.....m.zc.R.3F#...:.zt)..Y.[..F..9.[./cA.>m.o.>..MC.../nY.C.....0...f@..{...Z.t...jG..b....H..Z.:..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_Panel05_PriorityFeature_GetThingsDone[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, 1040x585, frames 3
Category:	downloaded
Size (bytes):	80543
Entropy (8bit):	7.934604031810399
Encrypted:	false
SSDEEP:	1536:0cQxZtUTe5zi2LtMuAJ5csKi0Oav3jMBsmBjTVHsW3KMBqR9Aeh:05xbUq5zig2J5csKH4SmBaW3KMMgeh
MD5:	7949AB2316B143F0F821FDB64378732E
SHA1:	1824FF40D53DD71B0F2EE9A6627B3B967B42AF6B
SHA-256:	A7AEB19A813C1CFAAF82D0F24C41FC624BE289C7C01475D6C3D8DFF566E4C4AF
SHA-512:	99A1A91EA4F3C37C8ADDC8B0F22FDBC5B83F031764D3588C23EB28BB6D723716C22BCC58AEED474AA9FE3BAD9006B9C404AFDB1A2610B09583A9F19E99B8F 21
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel05_PriorityFeature_GetThingsDone.jpg?version=26655609-1c29-c3f3-4795-badd817e0fb8
Preview:	......JFIF.....I.....Zc..')9I..NNC.r.4...L..L..$.R..b... .0Q.`....1.TTTTRH....C.$ND.".nRl.$.@..&.....$...Tc....F1...a.....E(....f...&.)9...&..&.I.....IE%....1Q.T.a...EF.*1.Q#. CM=.....&.'"L.&9.....`....W..K..I%.....1Q..#..1.c...F*1I$..... &..)...H.&.6.....w.wW7.E.T.R....E$.....*..c..0QPPQ.TR.QI.... .Cm....I..)..`....].]]F.8.!.p.)Z..*)EF1Q..c..1.c..1PQ..R.J"C@..&2@.....99.' C.L.....B0.c....(cb..Q....*1.c..1.c..1.T b..F"D@`..lcm.2NRs.....i.&k}fj1PQ..c..0.gh.J)F1QPP..c..B*1..Tc..Q.G.h...Lcm.rr..H.i.`.....1Q.T#..0.d$..Tb...(.B*.Q."...1QQIE!.i.wI..C%")99.m.H`&.....J.Q.T"...1.N.$..b. .c..F1..c..1Q.b.....@.....!..r.)..r&6.&.....%N...c..F1.i..QQJ1..c..F1.c..B1Q.b....J.+…n..:Cl..nSrrl.$.H.....]..a..1.c.....m$..Tc...EB1.c..1.b.....O'...m$i....nRr.7).A .....T...F....".n.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_Panel06_PriorityFeature_Security[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, 1040x585, frames 3
Category:	downloaded
Size (bytes):	101672
Entropy (8bit):	7.966199724517465
Encrypted:	false
SSDEEP:	1536:uZUPmA/MEynItoQtYPgognzJyJpXH9ewR8Y5qQwi895pEAqSsK82u3AafsyF9jqq:uZSonCvoglSpdeu8YeDpCSX82q3qVYyU
MD5:	770EBB154C0A43367A1CC212EDF18C94
SHA1:	B4304556D314B622E96064CB316BD34FCED2F0CD
SHA-256:	5B7404199463D38511324A09EB4200D3EC9B6E749863218EEF22226B09BBD911
SHA-512:	AC92422CA06140E4D778E10F19EE16332B35ACA3DC74585F182AEAC006E63A8C3A7DAFAAE7E9152CF5A18424B9761C1AF66A066B32B5CA1C74C6A2457C1492F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel06_PriorityFeature_Security.jpg?version=5e3f1a97-c694-90c1-e86c-675c1eefd82f
Preview:	......JFIF.....I.....wf.v}.@.....X.KJ]Kq..<X.....Q.D].>..u.iQS.o?..g.6.H.....,jIen..G\<{a....H .K.....I$...\|..o.<p...6..h.....~~5..[Z..,X..A.65q".E...]}..4.I}U>d...../'..3v..s.@.....-..c.....m....>...1..b.._,....-.TcA....>..7%.Yv-.x.6.....`y.]u.Mf>N...^...8...{Ve..3:..\|..d...O5.....j.....OJI.....K\|e,...''..m.\|._v.;/.{. ...\|..>^fvnd..Q.][0".a.8.....;*....t-.\|.*.....W.ek.#..b...71..2H!..:<..j..}.K.FNvw....j..G.ze....6..;`..\|Or..c.....z.....WO. ..\|.....~.Y.5.....[...>....Yrr../Kd..w.y.8...).p.y..w.m..Et6...:F.....Q.....;....$.v.b..Kg..A|.2{.....+;...)....u.U[m.c.b..m..~kd.~...w..y.....S..K)Lj[.[1...C.<T.x.t...K.....4.]\.o..:D.vD.v...2.8.2V.y....6..'|.2.|.z.....i.+"...+/.,..5r+m1.~...|.][.V....5..0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_Panel07_PriorityFeature_GamePass[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, 1040x585, frames 3
Category:	downloaded
Size (bytes):	194936
Entropy (8bit):	7.984735984852966
Encrypted:	false
SSDEEP:	3072:VPq1EfH4ipm/OpRBTr7/AUdjGwMac4+Ahcn6jBEWwNkUF3JzWzRk4uvHeA3:km4is/0jjZJGYEWwN3ZJ6+vd3
MD5:	3C2411D672DD60168176D3B62635AD4C
SHA1:	53D18AC4194069581949AB08781137F3FCE6C85F
SHA-256:	3C60463AC0955E563DA69B5D767654B5508BB596F848C39DD03E298ED88B80DE
SHA-512:	ADDF61092699862BB063CB417FAC389D44CD626171F83AA23B335D82B3EE17006D2CB2218E633B5DCFF2AB839DBCD3345A7443CA2120A46E1F6C6F6F2210C36C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel07_PriorityFeature_GamePass.jpg?version=67718e36-854a-a201-1dd8-12a68d406d7f
Preview:	......JFIF.....I.....L..&....P.....*'"%u*"'.."'"'''''....d.A....*..Z....R..,Y....vf...C!$...P..P..QQQ+J.P...V.E.....D.A..A.....u.u...c...^...5.B.....T..B....kTJ.T.$..Q.kEDEE. .A....(UTU....EPD.9gwk.....<0.....(P.**..'".!.(UDTDZ.k...A .. X..U.+....B..f.....[.1-!.....*..DUY....*.".'*.....Z....i..DQ....\..;Z.?.....T..."...!.....(...X..@UP.Z.]u.U5SMu"..L..3...kY...12@@...DUX.(.....@.P....UT...@..".Q.....h...DU...1v..f....$.....,X.....,d.(P....UT.$....E.B...U.QM..UU%b.....v{I....0.$"..."... ..392@..U@...B..A....,P.U.....)...Q`.....d{...0.!.E...H..C.,..x@D..h.....z(.....D...D.kDJ.....*....j...,.F.....0.4.L.. ..@ .....|U.*..XlkM...{..A.....&+I2.k-..{-.s.Yc.aiO.....UV.....<...2Ba.I 2...I.7...=.v..Q..,.&Fs>f.cv....5...z..8.:.I...v.DP.j..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_Panel09_4Up_HearingTool[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):	29813
Entropy (8bit):	7.98015026340844
Encrypted:	false
SSDEEP:	768:hpYp+TQWt1kB0/vQ9hcU3SvrfbuMCdHKQB5z75noAn1qa:DYp+MWiWySvHe975n31/
MD5:	46BC776ACF2EFB6A721AEC68798C8780
SHA1:	2FF7F13336540435D5A06DA8F91D4FE3914FDD87
SHA-256:	943CD3F7A7801A61C6D855DDE3C78CC4447DD3F556BC5120418ADD6AB0C749B9
SHA-512:	586E196C30749450962A522867A514F46636C9D6A912540D98ABB85DA3BC2FEF99A198FE328A72850BE72196BCA7E39E4DB1A53873EF26CBDC5449B27F97406E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel09_4Up_HearingTool.jpg?version=a25700ba-e0b6-2a8c-da8a-68dfbde01dd4
Preview:	......JFIF.....f.....r.H8.W.c....ih.....H..e/....i.q....!-.[6.W.s.,.....5...S.1U.0i6...v...0.>.j...6v.J=K.i.E.]..v...-.....^6w.:.xJh..?....C..I..>..-..s.yX=.'.}..V|..99Tc...a^.fU...QS.\.v.~.Nb.._.C+VU....:Q.t2`.....9.+\Jf.N}@..7.....W..WL.)cw...?A..E....X.kXs..$$...<.Nyf^@f....;.3o.b.s.>W.._}.Y.b.....'.a0qf.i'..$....d.!.4.....}..x...X_D.K..Z.g<..j.%.Uc}.5#.(...c.\|..\t.hQ0..wZE+>....>[..m.F.k.1~O.....H,.^H....c.u..2....>.].w.T.C...~.m.{.t..Wb.&.....R...@a.R.Z.I..}.(.C.....=Js.....K...W..$gn.+...m...O.R..... .o.}.U..H.....'..E.).';u.O.P.].C.k....>..}...PJ...]....0j.....(:N.....%..8KD.^.I..+.G W.9.Iz...R.v....z.JwH%....c..I.;{mU..!.-.....M....O..z...].1u.v...v.w...Tc&.4K.%.....ZY..q..u.A.+..0..a&A...W$V.7..0.5.}Y.}%[.,..e.r.L....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_Panel09_4Up_LearningDisability[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_Panel09_4Up_LearningDisability[1].jpg	
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):	21164
Entropy (8bit):	7.972291454252598
Encrypted:	false
SSDEEP:	384:fDAuYgj+VnKDcAjAP+7Kgmqb13F5spsROMnnn4owRDaIIyRxUpdIl0Y:ZIM1j6+zmwCpG1nn4PbxUL6
MD5:	40875D9CB2AEF302316728F02FA3B141
SHA1:	488C186A0DB2A9C96BC4D3169DC3E56AE5DF2E9E
SHA-256:	104E4A2A7445295C2DB1EFAEB50CC95D3F17D06D95437160C4D4832804B3698F
SHA-512:	30E130A984AF8D23EF255CAE6B0BDBAE3C846594C4EEBE300A6B0C091A34875DBE16EAC4BA59D48B803038CE61310ADC21286781BC0B09A03C080B7B94BD76 34
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel09_4Up_LearningDisability.jpg?version=9cb903d6-7593-4adb-62e7-7d3d2b1d68f8
Preview:	......JFIF.....f...../...$...}.9.}.e.[..L?..Z.B.%...W1o .O....F!.AB1....}...x.w~T.h.....}..K...w.....!....y9.a_:..|.nu?`g.th.O.$..U.e...1. .@!.).=..\....$..k.M.... .<4}Av".!.c.. ."...U.....h..Wr.k.....K=\....C..1.#.... .....i.......5l..u...8[1'.e....%... ...D....)F-&.j.o.#....c.Il..+.3....(@.1...B!....2-Z..'..\.D...yL.uN..ivV...(@..!.B....n..U.>id.y..:.f.7)`.?N]...JP4%... .BL...ZR.m.y..a$m..T.aN{.M....JP.!..B0."E3V...N.G.xY.Q.`Y.....S..... .%.@...!F.5B9J.r...X...U..n..T...c..R..(@...B..!.9:..8srq..!i...?..F.q.'.J.. c..1.g..^....`.+n...ou...}.c..R...@.1..?.H5.D../.1%9-..?M\M.'.....-5..q.cJv..o....OW1-...)Q.....=.....i....k. .....m.os....._n...{..au_A..._0.t ".}X...jk..PU\z:....Y-...so..../../...3jg...._:|."K.c.Mh.GXc..O..9.....O..-}..I$.e.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_Panel09_4Up_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, 358x201, frames 3
Category:	downloaded
Size (bytes):	25688
Entropy (8bit):	7.966149094108372
Encrypted:	false
SSDEEP:	384:fdeYmDj47zysyisSkjmJNPVtAFW8DUKv8YkaqGBtMgIcK+zL5K7m5KGlNSR8EA8o:lpyYn2WNdz8DUKUWBx2+8SgGPv3f17
MD5:	F414004523ACB5F130B35B68089BBED7
SHA1:	8218A2EAC55E16F0BF5EE2405A8D4D59E07422F0
SHA-256:	F65BDE6071BF29361D26BE6D2489B585AFD9F2A952736A560E379FCAA0C79EBE
SHA-512:	DE2D253EB5BDB641C209BACC035AD0F635888C81BB4637A8070D1C1700F9BAB98C6DD7F09895ACD58277874C131BCF5C2EF482BE1A6066AABA01B5EDA8F85 6B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel09_4Up_Neurodiversity.jpg?version=58c953a3-f516-82b0-2f94-398392076f5e
Preview:	......JFIF.....f.....(.d....;...v.:w..A....^...@...u.IR ...+^..Ia..JT."..DAl....._P..1U\.~,M.S.\.t..T....'Dwsy.^{.d#.fae...w.z..~.....W....."../..._..9&..\1.V...../.yC..n.A...W.3Q.y.. ....~..c..#.....2.j.6..x6a.....ku..%:...{..|...o^.....t.d;.R. ..gy...z}&..P.c...T%f...r...M.{.U.A.v.D.....N...GUr.."E....Y...9.....,....j<...)_)4~..n.....y1...aQb...8:.P.).....z.c..NG .]..4!b..t..y....zY.!.W... ...gX.=#.x/....B5.S].1..U+..~W....R.m .....o....<..q..v.u-....gC.=..b.q....].a...e6.\]..P..`.,;...&K.@...d..x....b${..h..9.b...CG.....=.....tI.).B..s...o....:G#..G9.z^....=|.+.....r..\n3..|y/+....S..U.....T...#.`....C..3Z...I.u. .B.C...D~...]..d.....=..b.z.#EI...i...0..w.n.i.....J...}Ok\..j....a.j.....y....B.8W...^c.B.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_Panel09_4Up_VisionTool[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):	22071
Entropy (8bit):	7.972488799944556
Encrypted:	false
SSDEEP:	384:f3WV0NopEFPaiXUDqe6ZkUVtUP8qT1Ty4R46tZheI1Eg0PSClCjcq:/FN1FPc+ZkUVWxT1T9R464Iqdls
MD5:	BC7AED9975732405BD166935D6A41EFC
SHA1:	A1240A865C9A0FBFBF59B8139806E4F48CA3C0C7
SHA-256:	5B580FA42DB3FB4729764E7D37BB31E48D6621B39F928EC22C6BF596734ED1B9
SHA-512:	C716DCAEB660E84D4339F1F23F3BA909B48FBC924E60BDC3D579DDA66D1AEBDF89C1574F220B7B87B9BDE437F9696F0ED12B300826E79FD85F4651592352943
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel09_4Up_VisionTool.jpg?version=f136feae-cc6a-f8c5-fa7e-3ba320f975d5
Preview:	......JFIF.....f.....F..~..).re..."x...Tj..k.n...T=...h J...s;....YUTS<.L,...PyX..k.@..S.3..(...M.Q...o.8Yu.QL..`..I...Pu..A8.....G...\:Y.....p.hi..@"m...=...KJ..j.e|*3.[.6MGyW3.....P...,.....c@.Fb...e.y.)U.....7N..d..B!....9.D.. ..w...i.l..6N...Qf..$...9-.8..d.#.5.....V.=w..U..N.Hb..u.?.c..XffP.d.M..=(RXG!l.=...i..a..t....a.C\T.g..%.kFU=.~=>....$.op..k.;...QT1..3.vy....as..jV.x.-.er...^...83/Q.I5=.r7.Px.{....n.R.... C. ....l.@....X.27$n<r...O.C'.#.*.$.\....:.-...6a.o.E.#3.;G4.Rv..{&.....K<).Q...j....?....".bY...w.....J!....0.)...eE.,.j gJl|..kKV.i..>!.F....R.!65[.U.e...N...$.4D...).=O[*.....+..+.%.~)V...|..h...q...b0.....+..'+.....)...~.T.....%...m.Z..4...Xk.$.4.....Wg...m.4~.\.V...>=1.62..D,BM.O[/.T.w...,M.X.+.*[!'

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_Panel11_4Up_Bring[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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_Panel11_4Up_Bring[1].jpg	
Category:	downloaded
Size (bytes):	33762
Entropy (8bit):	7.967880107239827
Encrypted:	false
SSDEEP:	768:8B4K+Tq+wNjAJZ2gbKqc/wsLrW7s6NyrqiRa789HK:G4K+TE6JZsMsXWqqiRa78lK
MD5:	2B26950F495614F8F0093C7D5CF546C9
SHA1:	1A32765F9EE01F623FB8097F9835EF60244A89D7
SHA-256:	24F6754F1131FAFB99E6BE1B2BE7F2C9A6C1B1C3063277E77572D7FD24CA1609
SHA-512:	6AB4C789C12EDB654759028B95F0DF9CB444F7C4DD6E1EAC48DB4F9BA202A20DAF0D45FA0F8BD6B40CC7291358603B8863FE177051133B7166CF79CCB81F87 0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel11_4Up_Bring.jpg?version=6dad2d9d-7e5b-403a-290e-4c009f855a65
Preview:	......JFIF.....f.....o...c{.mn{(...c.}.....i...w.2\..... .K.k._g.%q..1\.b..X$.NZ..z.....[..}.7.0.7cT.=G..;...6..tp.....jh.....j..."{.:2ca.g.....%+..Y.RQm6.eb..@.....jQ..zI5.!...|.>@.....X....H..p.Q7.J.....S..'...4A#za.B.....E...<.5.....[. .A#z].k.I.x..U.....C.....0.Msyx..XH.U1..d...k.n.jC5...L....V.oB..D.7..I./...H.V.....\.v..[Z.w.y.....4..^.A.5.o..f.~.....N..J....o....{Zi.4..X.....o....7.5.k..E.A..;...kz.z.....:..... ..9P[.:....~v.....S).U...@.64..-.^I.A#~i.b..}Y.y.5#.=\.~X.vot-..W].I..4.."SE.V...7..#jg.u_.n.S>.RN^...)...z6..T..*_.@.VH...8..../..e..M3.....jq.P\.#mxW]|...._^0.....+~_.h.J...-....r..Z.... 4+...L....5.i.....i.....PE..2._vmh..faoV2x..[.....p4.ux.4wOt..y1.+~f.M$+G.\....c...qB.....4IX.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_Panel11_4Up_Connect[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):	25325
Entropy (8bit):	7.961526581425028
Encrypted:	false
SSDEEP:	384:fz/kz/XZzx7jmMqXT53ThsHryhfDU9Mkfg9KM5suKlxLcpt2GcnqBtx17hdwa:YRxdqXlDWHryhflkfg9LsdrLstZ9Pz
MD5:	98A5534D064F59AE20CDBD268EC511E4
SHA1:	41C230B7B088CEA5D63D04C734FF117949BE2669
SHA-256:	C350649E8D2487A1EDCEB3A2C960BB2BB51377ACE42FE8236B2243CC588FF6F7
SHA-512:	7AB45C5DC9D3336CB6B178F70B1A55AABBD0ACEF5E40129805E84712C471235F0A7B089804BC3DEB912E4DB3B714CD1F04F07046640F9D38E1E1D7D5715FEB D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel11_4Up_Connect.jpg?version=f006d2a3-0493-ad44-261e-57c70c8a5884
Preview:	......JFIF.....f.....W=...Y....vce ..z.%@[.....y..Y?8... RP;...@...9..=..Jk.v..B.@..R3{g.....7...t+=*.,_....k..l..#...R..Q.r..V....C..v.6..^..z_.....LNnNl...}./...>.7H.Wk.....U...-.Q...8.T.....b...P...o.S*.....C.....T..E}jwk...s:..z...X....4+ .... .=....k....w@..r.|._."B?d..F.d....^.....%..+....y.$po}..w4+ .....2.6.$.G7....hV@)P.%x.`..e..s.tl./G.....c...g...d.....+.m.7.r.T..'R.|..w-/a...d.....;.x....}....z....d.....+ .....8....+k.....q...N. ...h.`..K....T.....7_E.{..u..a.<.3....B..J.xKZ..S.....w.9..oS..'.oX..F.d.....8.p?_8.9.9...a.s.....d..M...*..E^;-K{E...|..r ....Y..@!..6.9....+..p..N=I.}bd...c.l....T...V.;.n.`|.cS.7..t....oBc. t...Y..@1.?..t..}^...?.....@S..w..0.....~..x.].....'...r.....TV...d.....a.ll#_.....}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_Panel11_4Up_Organize[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):	25130
Entropy (8bit):	7.972294216006464
Encrypted:	false
SSDEEP:	768:jhfx6DSxhFFs5sLAcBDqF+XlqQru6+wbAR6:jhfdheLcBD4UlRCrAC6
MD5:	C5929885CA94723FB26195043F93396A
SHA1:	92247A850DFA048529C387CC9AA3B30453DF2425
SHA-256:	F46F50E5B4A3F0C7A47E73A9C04C94D224C2E3262E596B3714AB8D419BF554FF
SHA-512:	08E91764F4C98354BDB0FF553239883459970E339D24A745D7A08C13610BC5A9B283CD1B4DC70AD459349F9D51CE1C97F0C4C5717CCBC7CA1C08C79FCA53CA F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel11_4Up_Organize.jpg?version=89901e39-7dfb-9f82-820e-0748738660e5
Preview:	......JFIF.....f.....U.S.....>^....w..9.W.Q..(...._.. ..U.....`...v7<....8.O...^[..8Wq...;...}-....Y\.X..&X.a.%.:.Yg.....d...bl..z.z__.f.C....T....Q.>.?...e...v_.n.<F..i`....sY.9.....{.Y.....5.....B.8j..(..(.Q....*jOl._OMy..T.O._C'.\d .Nc.Xp:7P....h.R....9.$7..cz...\.-....d.>5.....)r.I...\$..:v.otX.n.|y..../=./.....3(p}.Oj^h...j..E...?.;]...y.L+Y.....Hs..:.....>.. ..2E.4+.....[h.....d.E...L..FF:.v"..,.fY....._5....}.]...[.tt...E.c.^.. .....t_..3.....'8.O..2Avm...k..Z...C.V...|.:.J..U...6...~..uH..y....)Z.'E.T..W..2y....ff.5.Xg.D.V7..J....+.../I..Dzx...}..X.....v.|...\....C2,3dy&^.....@.x/=.c...r.%..... .....Pggu.Q.....N... =.'E.lz.`.-...+..m,R.9P...)B)r..(..|e.4zM.V=c...r..x1.....U.}'G.v.p..4V.k.Z.c.G"....~/?..... *

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_Panel11_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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_Panel11_4Up_Protect[1].jpg	
Category:	downloaded
Size (bytes):	36343
Entropy (8bit):	7.976599466340477
Encrypted:	false
SSDEEP:	768:uFTsWmHDul50UfC1PRmTUQDQcWgb54DfGYKlNsA:u+300UfQZmTJDnWgb5JWA
MD5:	2CED0EF9918A9AFC1F80AE167E1EADF5
SHA1:	745C5891D508F921810A5F9FFDEC1372666F433D
SHA-256:	28BE9E2A8C74168CF2E529A51E50322EC938F2DADEE86A1963EEE07C78E43A81
SHA-512:	79566B7EF17703C9B6A0E95FF93B2D572A2DC5C5F6FBE5E331BC2D829341C4FF8C7CF85756F83527ED46D35C562595EA1F1EA0138690936C1CFE3C4F5C8436A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel11_4Up_Protect.jpg?version=fbfe02b1-43cc-8090-aa47-d36c4d6969ec
Preview:	......JFIF.....f.....K...".....{m.-.(.j.{4iF..... ..a.z.5.$.n.....cg.....T...6.L.~..B\B5..X.<..UR...,..3z..S....5.3.F..]_@.....ju.)..\t.2.<9.....N1.....u....~.....{...5...n-.J]...Gv..W...._.....<.[.}.x...Z..H..O ...K.....R.Gk._.. 3...pz../..[1l....9....T...'.....},._.l.{.....7r&^..b...5...=.....$k*...>+|s.V..6..*.\.B.V..J=.....,l...._as%...?....Oa.m<....>&d..i...-..ln..c.._W....N..3...m>.R0I.o(...ZDc7.2...._..qh...T.S.;.. .L...Y7.DJ9.....<ac.>.....Iau...Y._...-_UD!..kF_7..x.M...,...v.=..n.M....{...p..w.....i[.^.I5..I..%w..V'.....uSo<<..Z.@.Ui..t....B.....j+....n.t.jc.'..U.%.....,U..Q^.....8S.....o6..._T|.. ..M....?.}.....g...|w..hU../.-:.?.B\.....uk+.5-.C..,..W..+..nv.2.@.K.R7~jj.u..6.|..s...\.h....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\2-PlacesYouGo-01[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 370, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	118644
Entropy (8bit):	7.975720398535549
Encrypted:	false
SSDEEP:	1536:GRk+G/X80MKWyy6E62ETq5PasviPGEatsK2Hoc5CKR8EQVyQ5LbmH6vBTYmhMz+v:hL00MKCgAXiGsKC+lQMUmavlYqMz+aSJ
MD5:	030A9315A92BB58A3586B28B1CB61369
SHA1:	2EAFD5EF91D27E557223F3C06EC94D5099C44FE2
SHA-256:	272E8CE9123E9F1978ADFE83477481CBB8A346B2202C4F36264C3B399A7543C4
SHA-512:	65B1CDE76DCB2E0CA6C406AAFDCEDCA7915CE486095760CB12F3C64709E3B1471A5D9763D2369AB2F937064382087D4B7CEB05B7205B3782A15409AF1C9BF8F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/2-PlacesYouGo-01.png?version=47a491b2-4d89-d1ee-0918-a252337fe2a8
Preview:	.PNG.....IHDR... ...r.....).....pHYs.....8".@....$zTXtCreator....sL.OJUpL+I-RpMKKM.)..Az..jz.... .IDATx..Y.%.y.x...f.}.j.....@..)P"(.c.fd9,.B1.m..(.~...e<a...x..d..EQ.@.... .n.... {..r....3..D....o..^./:...f.=.n.....?..w..!D...W.....3.`}....o..W.....B.7.y...?;?..i.>.nl..b[..Qh5./8 t.....M.h.+...;...f.....?~.`..@.....^J$..U.-t]_.d..j2..G".E.....].....b.B....o.[..N.T d.O>m4..A.T8.....|..j.r....EEQ0....0.d....x.e.....Z.Z..(.m.ZcJ.....0.|P..ws$..\.`...$.../~;y...M...!.fsvvvjj.\.[..'.}..d2.....?..t...C..s....?.....?.#..7n.....s.....F.....g.....P.7W.*.bl.....,.c.V. ....*..3n...z.c.....9.W.G.n...._v..y..gX..6..?.?}S.....C.....s~..3..[.t.....g.z.z.Q}.cy....a.+..j....py=..+[7....|.aW...q.Tz..7.....o.=z..``.....J.Z....\.=.8.xB.../].D.I$..in.....I...x.as .\.Z.'..t.....K.Lflt4.Y.u}wc3Msii.\.....A...=.!..x\....k....X.!/...3...V.vw !.?....WAWk..dwy.M..z<.c.....Z..y.IC ..(.4....X,.h.....N.8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\22561495Platform_20200401_22561495[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	4242
Entropy (8bit):	4.869488209652324
Encrypted:	false
SSDEEP:	96:/91GclLjVCDvtsjSQsapFrcYn2R5GcHm6L8xazKMh0jThRKHzQ3yjto4vSKBJTmM:/9cclL5abbapF4Yn2PGcHm6L8xazKMh5
MD5:	C2A3DDF8E27595EC69431352399203AC
SHA1:	C752B6A26DC9038ADE9BF116032CB59CBC941A7A
SHA-256:	BF90FCA7309518C1686949E0F14C3DC1F430E169210F0C6A96E4209267A1EDA8
SHA-512:	5E4294F38A25026BB547CE0A460AC2E7FD73DD8664CD1A7F69C607087E6FA8EBB20A35C2772BA32AF295D14A5F5AE57ED4E4A63DC8EBAC782C45E896E2A584C0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/de-ch/videoplayer/resources/22561495Platform_20200401_22561495
Preview:	{"agegate_day":"Tag","agegate_enterdate":"Geben Sie Ihr Geburtsdatum ein.","agegate_fail":"Sie haben keinen Zugriff auf diesen Inhalt.","agegate_month":"Monat", "agegate_submit":"Senden","agegate_year":"Jahr","audio_tracks":"Audiotitel","agegate_dateorder":"dd.MM.yyyy","browserunsupported":"Ihr Browser unterst.tzt dieses Video leider nicht.","browserunsupported_download":"Laden Sie eine Kopie dieses Videos zur Ansicht auf Ihrem Ger.t herunter:","cc_appearance":"Darstellung","c c_color_black":"Schwarz","cc_color_blue":"Blau","cc_color_cyan":"Zyan","cc_color_green":"Gr.n","cc_color_grey":"Grau","cc_color_magenta":"Magenta","cc_color_red ":"Rot","cc_color_white":"Wei.","cc_color_yellow":"Gelb","cc_customize":"Anpassen","cc_font_name_casual":"Informell","cc_font_name_cursive":"Kursiv","cc_font_na me_monospacedsansserif":"Monospace Sans Serif","cc_font_name_monospacedserif":"Monospaced Serif","cc_font_name_proportionalsansserif":"Proportional Sans Serif","cc_font_name_proportionalserif":"Pr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\3-DataThatHelpsUsAssistYou-01[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 370, 8-bit/color RGB, non-interlaced

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\3-DataThatHelpsUsAssistYou-01[1].png	
Category:	downloaded
Size (bytes):	71404
Entropy (8bit):	7.975787790135017
Encrypted:	false
SSDEEP:	1536:GEk6h8429YhpiLgcNJJuwMkIfpr+t8PbvWF7/P4eHZjWwz:pZhYSiLPMkIB62PbvG/gSW+
MD5:	949D1F10E2BB814BC19A20217D6B9EA1
SHA1:	18DA18B4D629E0C4960B8269AB28F2513E7666EB
SHA-256:	5E585D7B11E11A0A670AB80A8F8E5ECEF89CE95DC93F070EDC90D98B0EB98B36
SHA-512:	705ABD496324ED20524CED830F1D762BBA4750396611AF83C961DBAD48EAF248026A51CC6123D8E44D2D6A2D6B68BEAD44F0A7B2D7B259EA9EEFDC0DC95D4E9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/3-DataThatHelpsUsAssistYou-01.png?version=7e8ad63a-46d7-7f13-d54a-f8fc1d5efc47
Preview:	.PNG.....IHDR... ...r.....).....pHYs.....8".@...$zTXtCreator....sL.OJUpL+I-RpMKKM.)..Az..jz.... .IDATx..w\|....g.l.....Z..W.5.....lp!1$.B..\~.\..7LL....@..P..0.)...-... eW.?...EXm.....K.y..)..V...z.#$0F.!U...+....d.(D0.0V4.OPj}.'...6..3.!.....&{"S...`.X ..}>w..m.555..w.kii.f(..n.U.VA.UU.o..>+I.. 33s.M.....>.h.].....u.]...._~..'....+W.....Vkww...?.... .E}....g...O~r.....8....*...../4...h...Y\|.F...1..1.&{.Q.,...e.a.0....y..s.pDE}...D.R... .V+..}}}..N.t&..a,..M..}....e.....~0CA..,Y.a.....Ow.....y...n...I..(.RRR...s....9.s.....7...''...<..S. ..E..q.=.,].....?...'5-.....}.....!..\|.1....1.1RUI.}."i..P..{....t\....SC.....`..n..\|>...a.[..0.....i.^.v..k.....L..`F.h....}...~.m.../.x..v.].}..=..3. .4.z..k.2.....<.o..[...A..N..cG]]...(.. ...x....~._tww.~,..B...SZZ:X.....b..l...A.....#....."!.....i.}.. ..$.Y.z..&{J....l6. e..`0..f. ..|.y.m...].n]{{{0Cq.w.7^{.$|''.^x..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\35204097Platform_20210602_35204097[1].json	
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):	3931
Entropy (8bit):	4.8079273430772025
Encrypted:	false
SSDEEP:	96:JbXNfza6QXVCDvtHwjavQg5xXVsryRyAcgo039V768KLaa2KATNp6+/QX4PZNwTc:Jbhe6QFaHxvB5xXVsryoAcgo039V768X
MD5:	2113FF57954680F90A4CDDD5A616F83F
SHA1:	5559FC2270328D3962FDACB108519786192B04BA
SHA-256:	07BE01E5A83F3D70C4D9B22FDB1F00BF0EADB88EF97C548E7122C7698D1A972E
SHA-512:	2475022E61CCD996B77435FCAAB3361EAB53221EA1D2AEB8CFD637064236964C9E95B3A685713D192D394A4CEF6DED801915AF64E76A85582518D068DA9F4B6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/en-us/videoplayer/resources/35204097Platform_20210602_35204097
Preview:	{"agegate_day":"Day","agegate_enterdate":"Enter your date of birth","agegate_fail":"You may not access this content.","agegate_month":"Month","agegate_submit":"Submit","agegate_year":"Year","audio_tracks":"Audio tracks","agegate_dateorder":"m/d/yyyy","browserunsupported":"We\u0027re sorry, but your browser does not support this video.","browserunsupported_download":"Please download a copy of this video to view on your device:","cc_appearance":"Appearance","cc_color_black":"Black","cc_color_blue":"Blue","cc_color_cyan":"Cyan","cc_color_green":"Green","cc_color_grey":"Grey","cc_color_magenta":"Magenta","cc_color_red":"Red","cc_color_white":"White","cc_color_yellow":"Yellow","cc_customize":"Customize","cc_font_name_casual":"Casual","cc_font_name_cursive":"Cursive","cc_font_name_monospacedsansserif":"Monospaced Sans Serif","cc_font_name_monospacedserif":"Monospaced Serif","cc_font_name_proportionalsansserif":"Proportional Sans Serif","cc_font_name_proportionalserif":"Proportional Serif","c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\5-InterestingAds-01[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 369, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	28305
Entropy (8bit):	7.959019315288655
Encrypted:	false
SSDEEP:	768:RqdkxbaId5ummUb1W/E3J3M/2f/MhQQiI1clRwLI:Rx1aid50Ub1W83M/2chQz6EwU
MD5:	F8D0DC34CB1C64F2FC93033ADF52AAAD
SHA1:	FC23B43FBC2977D9A729EF0661F1B38CB08B1984
SHA-256:	94BD6616569E965BDC4C413CBF8F67EF0FBDFD764648922DA5B0AFCBDCACB13E
SHA-512:	3F946D983C048072B3BE7F5B7C8D5921ABC04579051E355C55E77FF430AC130BE5D010B08D893D91C40C4652F5A39BB8749C75CB47B79FCBD5E88B6181964749
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/5-InterestingAds-01.png?version=c6f7fa36-8442-76d8-9408-9a365e8a26b5
Preview:	.PNG.....IHDR... ...q....._[D....pHYs.....8".@...$zTXtCreator....sL.OJUpL+I-RpMKKM.)..Az..jz.... .IDATx...g.].y/.g.]N.3U.$.....!...T.....Brl..S|.o....&Nr.a.....L..@.L....w .k...3....^..~x1s...9...*.".x.*..\.....".X.9}}}_...2?..>..O}.Sy5.-c..M..0.h4Z.c...(.R.c..Z.....5....P.ST.~[.~.....?/..QJW.X!I..O.w..zM..&O.C...^....?m;.Ch.gF"..0J..J...'...U.q..4S_...Yb... .y.P.8....!TSf'Q...X.!...9....gb`.H&.Y=..X,V...W.....m.q.{d..Z.$I.z..e9.Sq....!..655%..H$bYV.[tF.....^.. ..BH*..o..!..3B..(.R.u+1`.PJC.P0.L$..s...5.....T...W...x<...!TI.$544Tn.". PJ.Eq]..R.....LU..)I....QhY+.$w..B.S..+.KR..+p&.B.!..R3.*1`.Bf..B.!.P...|.$Ub...b.*.!.N.....Y...B....e9.a...eY...#..Y.....q.O.y<....r..!.P!...~d..r.....v.x...N.i.0.....y...2..h.....B..R9.F.f.r!.. (.@ .f.\|`.,B...EQTU]l.^9..$I.....{..>7QOU..P....$....dV.|.%.[..i....I9.,....[.vmA..rcY..Tv..!.P.e..]...l..... ..[..-5...._es....4..a)....X..!..B(si3Ly".,.K.....u.,..B..RE:+1`QJ=....l.....g ..SE=E&..5.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\6-SigninAndPayment-01[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 371, 8-bit/color RGB, non-interlaced

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\6-SigninAndPayment-01[1].png	
Category:	downloaded
Size (bytes):	78912
Entropy (8bit):	7.978996167181678
Encrypted:	false
SSDEEP:	1536:uzBi/whJc5DQcy5JX+wBGPhO8+8UtUvjcUCoSu0LL4TgbKfNcKjFT9:uzB9Jc5DQcy+fpO8PLcUgu8PmjFT9
MD5:	2C92ED67778825C64FE7A6A5CC1FA0FD
SHA1:	9915BD644C87EE22E1D0790113D6F7848AB1B4FD
SHA-256:	F9E1B0C44E8E4F5B2C2F7A2061FE415B1F1BDE35FFC8AF58478C55D5599D925B
SHA-512:	52C6929C03F686743F7ACF0460F6C1D1F17DDD72D128B5138B0C72B72614684EE2F3CBF8D6C3698B3EB7191C224965909922B15B40D754C2B08E60B1368298C6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/6-SigninAndPayment-01.png?version=6a1ba4d5-f07b-a8e6-3060-0bfa18dd42db
Preview:	.PNG.....IHDR... ...s.....I..O....pHYs.....8".@...$zTXtCreator....sL.OJUpL+I-RpMKKM.)..Az..jz.... .IDATx..wp[W..y..9. A.9.T.rv..e.[...N.jv.u...vk.....P./.y.3....m...$[.m.. .,1.9.D....@.h.").$...W.L.....=.{~.....[..:O0$l.t:.ZMQ....W.R...$.....9.i.jU..z..B8.!.....F....$<...G/w..iI....\<...tZ.....plw}u1B.?..`....;_...k|*"..~..&dT.h....,.5/&..[..Y..}.wS...;....s.....@ .G..7....a,-..}...\.m.#_..m.K<....zG...?.....~.,....x._..+.....B..t:.....{....hN.....).U.4.q...X...2.....&..B..N...;H....g.....Dq.x^ZZ.w..w*.j..I..N".8.M...&b0.....h.d.....M...$..3$lj4..VK ..\U.r,0.....zrp.O.W.|.BJ...y.R.y.....E.:;[f..5.?...q.S....!...b.....PWic...,c.7x..o.tcl2".Y....F.....& ..U...Y9H.,+++**...jkk..|....).8N(<..4..H..b....-"..^z..o.p....-D.....X..yU8M....e...0. C..4.ML..d.J..E.d.....D..P.T..F.P...+...N.$K.+U:.x.@,..9.6..ikY....U....FA..i...\..+a..]...9iY..B.sk..^...SMj.<!.H4....wO..6..7...FE...c..5.....z.`Yv.....}}}.x<.....1.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Acl1033[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	19181
Entropy (8bit):	4.3590974373798
Encrypted:	false
SSDEEP:	384:im1leaXgjDSEcE+fg1gKzqF9meWFaUOKco5FXp/kf/oezD:b1leajD0kiDlgMJkly
MD5:	D9604CC18F364A6ADE707B7FAAEC642C
SHA1:	F38F0B94764184D4373886FDA1CA87D352BFCE5A
SHA-256:	F282423F48F12F56419363384F3B10002C8D3D106BC1AC8FF721602AA2B2FD9B
SHA-512:	7B305607B79F077539E3C37CD46EAFBB9E4C9B2A8825217187515CD20FFBFE204BAC43E918CD4440EB65A3A2DCFFC4140D06B43845613D48566448765B3D5DF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://onenote.officeapps.live.com/o/App_Scripts/Acl/Acl1033.js
Preview:	.var AutoCorrectList={"(c)":".","(r)":".","(tm)":".","...":".","abbout":"about","abotu":"about","abouta":"about a","aboutit":"about it","aboutthe":"about the","abscence":"absence", "accesories":"accessories","accidant":"accident","accomodate":"accommodate","accordingto":"according to","accross":"across","acheive":"achieve","acheived":"achi eved","acheiving":"achieving","acn":"can","acommodate":"accommodate","acomodate":"accommodate","actualyl":"actually","additinal":"additional","addtional":"addit ional","adequit":"adequate","adequite":"adequate","adn":"and","advanage":"advantage","affraid":"afraid","afterthe":"after the","againstt he":"against the","aganist":"agai nst","aggresive":"aggressive","agian":"again","agreemeent":"agreement","agreemeents":"agreements","agreemnet":"agreement","agreemnets":"agreements","agressive": "aggressive","ahppen":"happen","ahve":"have","allwasy":"always","allwyas":"always","almots":"almost","almsot":"almost","alomst":"almost","alot":"a lot","alraedy":

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Enterprise_Trust_Center_32x32[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):	437
Entropy (8bit):	7.121498449889634
Encrypted:	false
SSDEEP:	12:6v/7uNp0RvmAf9vDBO3rwx8oAW7Fbbicpojq5:nTgmmNrxNAW7pbi2ojq5
MD5:	F710BE24875D1BD47725BE7B5E86281C
SHA1:	15BC09A3B55B96B7F5BD38D6F499173B294EDE42
SHA-256:	404B1F8A226DFFCF14D55323D8D06FE38A5500B31B7B867FC2EABA5BA5888ACD
SHA-512:	258B5261EB685A15CE114AC0E65392719592CF28BA560A241B3D66CFAEA3AE08D92E0FCA58B0E21053B78AC980F327FB2C9EFA885048CCBB8D35459EF05D39C 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Enterprise_Trust_Center_32x32.png?version=834fa58d-e8bf-02fb-f02f-0ad23b0a0248
Preview:	.PNG.....IHDR.....h6....tEXtSoftware.Adobe ImageReadyq.e<...WIDATx.b...?..\x.c.....}{..7.. ...o-h ..W.....S...B..#o.?....2.\. P..."..Qm0.~..gpQd...J..@dA.....@.@e .@{..b5.....G...P1.O.l.-..%n.l.....h.J.....@..D.....e`...W1...\..ATq.....K\.....O..J.c`..........Cw.04..=A.....q..Z.%.C$.8. fCD>...d...!.....|.....J..7..G.r. <].|..O.w..2.. .@..O... ...L8...Dx40.I...50...`.+../w.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\FavIcon_OneNote[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 3 icons, 32x32, 32 bits/pixel, 24x24, 32 bits/pixel
Category:	downloaded
Size (bytes):	7886
Entropy (8bit):	3.675002721266739

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\FavIcon_OneNote[1].ico	
Encrypted:	false
SSDEEP:	96:HOmS/+CtmE8mmmmm08mmmmmtf8mmmmmO8mmmmm+8mmmmmo8mmmmmo8mmmmmSC3on:AGHFk
MD5:	7A7A4890CAAA77025E1B33A6D6E474EE
SHA1:	DC735B99D9EF0C76B4A7AEAE8BAA4CBD9551BA77
SHA-256:	9E1DA5BF715135491519A188CAD977DB6CBA414071E2407B69D63221379D8802
SHA-512:	291692981A555857F95A3378B511E27B60154B95EA0BA0452B3A5536D9A63A16B00518066E4F4B60E6A73CBD2A7C46B99A18102EA5970989B9736E57A6474D30
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/resources/1033/FavIcon_OneNote.ico
Preview:	....6......... .... .h...f...(... ...@..... ....d...d...d...d...d...d...d...d...d...d...d...d...d...d...d...d....w...w...w...w...w...w...w....................... ....d...d...d...d...d...d...d...d...d...d...d...d...d...d...d...d....w...w...w...w...w...w...w.................................d...d...d...d...d...d...d...d...d...d...d...d...d...d...d...d....w...w...w... w...w...w...w..................................P...P...P...P...P...P...P...P...T...d...d...d...d...d...d...d....w...w...w...w...w...w...w..................................H...H...H...H...H...H...H...H...H.. .\...d...d...d...d...d...d...d....w...w...w...w...w...w...w...........

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Government_info_req_32x32[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):	252
Entropy (8bit):	6.641255724122932
Encrypted:	false
SSDEEP:	6:6v/lhPmNp0WnDsp7mAM2qawQ3nmU7B1PpmC2Joo6Cw+bp:6v/7uNp0RVmAMcws7DMC2StCx
MD5:	32B87D5E6F3876E0BC93FCCC9F1EA04E
SHA1:	0510D6D1B0834643731F2FD29089CED919A43551
SHA-256:	DD197BEF9E8E8CB7C17CDEBDA0712DE0B4FB0D959ED44D1668BC5370518D98D3
SHA-512:	1F1ABFCB4CF6402B08DD36E1CB19824C3F205252C421A91D9452EF72315F4FFFFEEB2ECE45A15011CE8E387833ADF4CC38C3B4F9D415D39B0AE7841EB9D426 A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Government_info_req_32x32.png?version=a9596e72-c98e-ba4b-86a1-847d4ab1f253
Preview:	.PNG........IHDR...............h6....tEXtSoftware.Adobe ImageReadyq.e<....IDATx.b...?.)..S...o.k..I.....g?....`..@6.m..`.....*t........."@q.,\...Rd......:.>...r.P..$.01.........Nz@...y...... ._.9.>b.U.ny.Q..L-....p..A....Dj...0.. .J?.^k....IEND.B`.

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\MWFMDL2[1].woff</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>Web Open Font Format, TrueType, length 11480, version 0.0</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>11480</td></tr>
<tr><td>Entropy (8bit):</td><td>7.941998534530738</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>192:QNhlpX236n8/cliy01vRGeJsqVZJZmKgiiwEkyaGG1QfPujdI5v9QtAOcAue2HCZ:QnjX23W8UcvRaqVZdgiiyRQf2+5v9Q0q</td></tr>
<tr><td>MD5:</td><td>5ED659CF5FC777935283BBC8AE7CC19A</td></tr>
<tr><td>SHA1:</td><td>A0490A2C4ADDD69A146A3B86C56722F89904B2F6</td></tr>
<tr><td>SHA-256:</td><td>31B8037945123706CB78D80D4D762695DF8C0755E9F7412E9961953B375708AE</td></tr>
<tr><td>SHA-512:</td><td>FCCBE358427808D44F5CDFCF1B0C5521C793716051A3777AAFDE84288FF531F3E68FBC2C2341BBFA7B495A31628EAB221A1F2BD3B0D2CC9DD7C1D3508FDE4A 2F</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://assets.onestore.ms/cdnfiles/external/mwf/long/v1/v1.23.1/fonts/MWFMDL2.woff</td></tr>
<tr><td>Preview:</td><td>wOFF.....,.......NH........................OS/2...X...H...`JZxhVDMX............^.qcmap............ph.cvt ...l... ...*....fpgm...........Y...gasp...|............glyf...... ...7.oV."head..'X...0...6. k..hhea..'........$....hmtx..'....v.....F.Eloca..(..........Y..maxp..).... ... ....name..) ..........b.post..,8....... .Q.wprep..,L........x...x.c`f..8.....u..1...4.f...$..........@ ....8.|...V...)00.. ....x...S......._..m.m.m.m.m;e..y.~.......<p..a.0t.&...a.pa.0B.1..F...Q.ha.0F.3.....q.xa.0A.0L.&...I.da.0E.2L....i.ta.0C.1..f...Y.la.0G.3.....y.|a..@X0,.....E.ba.DX2,....e.ra..BX1. .V...U.ja..FX3.....u.za..A.0l.6...M.fa.E.2l....m.va..C.1..v...].na..G.3......}.~a.p@80......C.a..pD82.....c.q..pB81..N...S.i..pF83.....s.y..pA.0\.....K.e..pE.2\....k.u..pC.1..n...[.m..pG.3.. ....{.}...@x0<.....G.c...Dx2<....g.s...Bx1..^...W.k...Fx3.....w.{...A.0|.>...O.g...E.2|....o.w...C.1..~..._.o..08........?..0$........x..AHTq.../..$mk...E#.L.<.X,..D..P..:T.$Y.x.*...!.u...!J..(.X</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\MWF_SocialFacebook.png[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	469
Entropy (8bit):	5.368803468427014
Encrypted:	false
SSDEEP:	12:tvG1W3aA/QU2Z9Vflb9WbrCrfdo97LCcnwiA:tu1UQZ9/b9WbejSVwiA
MD5:	58064C0EDB5F8C89D1C066A50AF5ED7D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\MWF_SocialFacebook.png[1].svg	
SHA1:	CB7B81145B59B505B74ED3507464201AB4BFF621
SHA-256:	6CD47E002200FC07167C3D1552C5E84693412784AE15B039383F4607A6DB08E7
SHA-512:	11A214A9A9DF47901D5BE6F867A7A2E739825CE12F98FD28755C16ADF1AEF1783E4082C6F89D9D522823458AFFC9CD60D070C27352E88A0A24F70545C17B340E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/MWF_SocialFacebook.png.svg?version=ca2b09b7-dabe-cbfb-0459-457c6ac59270
Preview:	<svg id="Layer_1" data-name="Layer 1" xmlns="http://www.w3.org/2000/svg" viewBox="0 0 32 32"><defs><style>.cls-1{fill:none;}.cls-2{fill:#231f20;}</style></defs><title>Facebook-neutral</title><rect class="cls-1" width="32" height="32"/><g id="_Group_" data-name="<Group>"><path class="cls-2" d="M17.53,26H13V16H11V13h2V10.48a4.76,4.76,0,0,1,1.21-3.29A5,5,0,0,1,17.88,6H21V9H18.91a1.5,1.5,0,0,0-1.17.57,3.53,3.53,0,0,0-.2,1.37V13h3.12l-0.36,3H17.53V26Z"/></g></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Manage_Privacy_settings_32x32[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	604
Entropy (8bit):	7.536558126606159
Encrypted:	false
SSDEEP:	12:6v/79GBuJHkED72vr7ExfqmQ2o6OXnzf9/GJAS3lz:yHku72vrgxfqfBr9/GJAYlz
MD5:	C382E6FAD96C9E69E6795F3451FD0D9A
SHA1:	0E96CD85D7AE71F252FBA327708BD7CA41E4621D
SHA-256:	3AC82CCBBF89BF84554E890BB73A523B1D31060D6DCD12A266C1691FD6BC4FBA
SHA-512:	394CE57DCD63009DA046F602047A39867E0BC6D750A538DE8C2623E564A4EFD87597CA91321AA9A0A3CC5C073462FEDD54AE542CD8D5E03E6A4ACD292CC5F A7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Manage_Privacy_settings_32x32.png?version=3fbd39e2-6e0b-de4b-17bb-2367d41e5f5f
Preview:	.PNG.....IHDR... ... .tEXtSoftware.Adobe ImageReadyq.e<....IDATx...K.@.....R.."Bqt*:.Pw.....N.....R...'].*..).E.._._I.iK..9.5yw.....`.\.xj'w.....{..h.;>.37..W..=.\fK./.. .".1.....>.z.~pyq<.NX...<a.....0n.....=.#.^...5Ggj..x.!.r..}V.F.;..`...0.k.UT..}|..x...Xd..\.....iF.9,.\.@..%....,qqD..V..-.h..,..^...$Pz.1.....8..mt....C...B}.T.....4.o..Ou.....K.....-..- O5..}~Z.t.....y...<.....?..{...b....C.U..ko.f/.....h..k...W.|.W.....M..S.?.) /B....tS@.S...S..,n.L...G$....|..v.[=..>(...W>~)..q.@G..k)..WoR.).K....?.....x.<<}....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Meetings_manifest[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	89749
Entropy (8bit):	5.907896932868388
Encrypted:	false
SSDEEP:	1536:TF7qkDiiBSPqAYXUJqc9a/qc9aJyXUEUx:J7j7B4S6RaVC
MD5:	1BF11FC2DBDB5C48B7D60F5005583417
SHA1:	DF52B131F6B151E674204CBA77082EFAEFBC3F8C
SHA-256:	172E218E70CC419328B7AAB580615DA2A562E1508EAC9AC3014C52C51F2F50EC
SHA-512:	A40545B0B88AAF5EC4D28015B72451CE6F19073FC7E1CF6A8B08EEAB6D173CCE9E62553CACFDA7FE0FB4DDECB2E09E8B966C6466AE50AC31193481D82898E CB6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161411141024_resources/1033/Meetings_manifest.xml
Preview:	.<?xml version="1.0" encoding="UTF-8"?>..<OfficeApp xmlns="http://schemas.microsoft.com/office/appforoffice/1.1" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:bt="http://schemas.microsoft.com/office/officeappbasictypes/1.0" xmlns:ov="http://schemas.microsoft.com/office/taskpaneappversionoverrides" xsi:type="TaskPaneApp">...<Id>90da59be-5361-4260-9218-2262af1dc334</Id>...<Version>1.0.0.0</Version>...<ProviderName>Microsoft Corporation</ProviderName>...<DefaultLocale>en-US</DefaultLocale>...<DisplayName DefaultValue="Add Meeting Details">.... START STRING LOCALIZATION REPLACEMENT (StringID: OfficeAddIns.Meetings.ManifestDisplayName -->.....<Override Locale="af-ZA" Value="Voeg vergaderingbesonderhede by" />....<Override Locale="en-US" Value="Add Meeting Details" />....<Override Locale="am-ET" Value="..... ...." />....<Override Locale="ar-SA" Value="..... ...." />....<Override Locale="as-IN" Value="..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\MicrosoftAjax[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):	108563
Entropy (8bit):	5.336815172511868
Encrypted:	false
SSDEEP:	1536:MGLiogSomRYvoGtT+KHsVS0bT79DSsi46j/LPyR7kmE1cRV:MGLXGFKT79DSs6WBEeV
MD5:	A21C0ABF7393D61292329E12D992DD60
SHA1:	B4B6386EC4371294F9C122E5479FE0110531D969
SHA-256:	4DDC354F0F9CEFBE066F62418B719E96AB7A788249DBDFC3AA570755AB5C3171
SHA-512:	60B82E625A8EF550834BAFF38934FBC5C1EE317462D0B4924C4DC92A2D9F1A9D6B11571B0ABE5D4B84F196297D98295FE9ADF3A128AB1071EBF998B845D55BC 2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\MicrosoftAjax[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-officeapps-15.cdn.office.net/o/s/161411141024_App_Scripts/MicrosoftAjax.js
Preview:	//----------..// Copyright (C) Microsoft Corporation. All rights reserved...//----------..// MicrosoftAjax.js..Function.__typeName="Function";Function.__class=true;Function.createCallback=function(b,a){return function(){var e=arguments.length;if(e>0){var d=[];for(var c=0;c<e;c++)d[c]=arguments[c];d[e]=a;return b.apply(this,d)}return b.call(this,a)}};Function.createDelegate=function(a,b){return function(){return b.apply(a,arguments)}};Function.emptyFunction=Function.emptyMethod=function(){};Function.validateParameters=function(c,b,a){return Function._validateParams(c,b,a)};Function._validateParams=function(g,e,c){var a,d=e.length;c=c||typeof c==="undefined";a=Function._validateParameterCount(g,e,c);if(a){a.popStackFrame();return a}for(var b=0,i=g.length;b<i;b++){var f=e[Math.min(b,d-1)],h=f.name;if(f.parameterArray)h+="["+(b-d+1)+"]";else if(!c&&b>=d)break;a=Function._validateParameter(g[b],f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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:5m73jcJqQep89TEw7Ukk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false
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\0W10PBUV\OneNote[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2968653
Entropy (8bit):	5.613142140363839
Encrypted:	false
SSDEEP:	49152:a8pBhW1t52yTBiRgwhaUVVyUAPeAAlAArEfKUZBUF6gk5VKEQfP2754KDaG1xkLu:5STqAAlAA0z
MD5:	EBD4A0A0DA5FD2476869FED5ACD7214B
SHA1:	93BB081D3A5746650E6C08FFCD861760627C304E
SHA-256:	9654062C04FAB60CF0D9F4BF41554B9E6EA5C98FAEB6C833F285E8EB5C494C39
SHA-512:	DEAA74DCC33AF9AF375D09E3C92A9FB5463AC751A98DD4EE9E7874D8C62B32400157DAA2040F68D0C676F712AD53DF5D6C769AF8405415D0CE32D3AE8EFD28E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161411141024_App_Scripts/OneNote.js
Preview:	var wac_aaa={};function wac_a(a){return function(){return wac_aaa[a].apply(this,arguments)}}"undefined"==typeof IEnumerable&&(IEnumerable=function(){},IEnumerable.registerInterface("IEnumerable"));"undefined"==typeof IEnumerator&&(IEnumerator=function(){},IEnumerator.registerInterface("IEnumerator"));"undefined"==typeof Sys&&Type.registerNamespace("Sys");"undefined"==typeof Sys.pt&&(Sys.pt=function(){},Sys.pt.registerInterface("Sys.IEnumerable$1"));."undefined"==typeof Sys.Ez&&(Sys.Ez=function(){},Sys.Ez.registerInterface("Sys.IEnumerator$1"));Type.registerNamespace("Diag");var wac_aa=window.Diag||{};function wac_baa(){}wac_baa.registerInterface("Diag.IUlsHost");wac_aa.lgb=function(){};wac_aa.lgb.prototype={};wac_aa.lgb.registerEnum("Diag.ULSTraceLevel",!1);function wac_ba(a,b,c,d,e,f,g,h,k){this.Zfb=a;this.bLa=b;this.Jv=c;this.Po=d;this.tm=e||"";this.vOa=f;this.abb=g;this.jq=h;this.rwa=k}.wac_ba.prototype={Zfb:0,bLa:0,Jv:0,Po:0,tm:null,vOa:0,abb:!1,jq:null,rwa:null};function wac_ca(a)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Panel02_QuickLinks_Icons_Deals-1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 193x150, frames 3
Category:	downloaded
Size (bytes):	18012
Entropy (8bit):	7.95075976461495
Encrypted:	false
SSDEEP:	384:+Mj17kaajk4y+AOfiTMPtn3DX2fii7UN0q3HKqJlgx40meIsr+27opA8n9O:+EpNKk4XffpnTX2fINH3H5543Fk7opO
MD5:	EE23688D8B481514AE3CA9A17F20D5DE
SHA1:	D5564D4E354601D3840CFD8D0E80E3BBA16C0FA7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Panel02_QuickLinks_Icons_Deals-1[1].jpg	
SHA-256:	77647A788B7E4B873E17684C93C930C329C04F2A202D5900B73923590E74447A
SHA-512:	1C8319CAF7DD2FAB64FA84E9309C8A843D71AA67DB1AB694C3567AF0D3A19FCA0FFB917A08F58FC4978BE466B88DB844B23E9ACE1B0198B86FF9AB3C5C0E41 20
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Panel02_QuickLinks_Icons_Deals-1.jpg?version=8d0d733c-3989-4055-23e7-4c32adff8dcb
Preview:	......Exif..II*.....Ducky.....d.....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-c006 79.dabacbb, 2021/04/14-00:39:44 "> <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:OriginalDocumentID="xmp.did:89694450-53d8-416c-aad6-852c8310fa46" xmpMM:DocumentID="xmp.did:F4572D36C0C611EB8CBF9901C688B737" x mpMM:InstanceID="xmp.iid:F4572D35C0C611EB8CBF9901C688B737" xmp:CreatorTool="Adobe Photoshop 22.3 (Macintosh)"> <xmpMM:DerivedFrom stRef:inst anceID="xmp.iid:b33c9cca-09cd-4569-a7ff-56bfdfb2d1a9" stRef:documentID="xmp.did:89694450-53d8-416c-aad6-852c8310fa46"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\PrivacyStatement_32x32[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):	423
Entropy (8bit):	6.978970659748671
Encrypted:	false
SSDEEP:	12:6v/7uNp0RzV2msPjjZCVhUaGOpoJYKsFI:nT6V2msrMqOpXO
MD5:	F6AA4887DB2B9713C39861B5DE1594DA
SHA1:	CF97DDE51731EB48403ABE27C8D0E7BC6E3A775B
SHA-256:	19917FF9E0FBA8CD1D86DB3417F4201B4CDA820A93C6B707F6D48EFA1308C701
SHA-512:	09FC7C213A7158F85988ACE8F40202D8863EF4075F2DB7FFDEC4A29A03CE4AECE4689A3553BF00AF7E7DF1AA9A622E31F4628A1D8CB7E7BEDCA81128C80562 F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/PrivacyStatement_32x32.png?version=0c5aa48f-df47-8af7-7c65-d32dd84ec9c0
Preview:	.PNG.....IHDR.....h6....tEXtSoftware.Adobe ImageReadyq.e<...IIDATx.b.....|x.....$.V?."8.(.W.....k.....R....L0....8.....drP..".d.j...d...k....!f..@Ad5,.` ...$..Y.....@... .?.Bm..$.p.?^.T.....t.".D.....U.....69.?.^.*._...3..}\|..7.B....'.....3.5.Hr....2.b&`8.,".....3....nyE...2.bhL;.z..Q..(.T..ihZ.p.].@...x..y .....\_6^..tL..p...P.....(...gHJ....-^.....z.$P5. .@.....C.t.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RC0238d8e49fc8405f878b79a26e794e4c-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):	1777
Entropy (8bit):	5.524571607264139
Encrypted:	false
SSDEEP:	48:Dwt/BuxXuxiSUYxUJxBotu11vlxTmBEfBaE6Oen9VGxhBHBENH:MBBWJdUu11vaBia5OiLatBK
MD5:	AB795BC8C5A46431500A5D57F82D5FBC
SHA1:	E3325D1BD293FDC1017BFED3659631269DC96D77
SHA-256:	0733DD4AB6B7ED8C52A5DFEE5C6D40D718E91FC29CB763D153CCF35C7AF37D2E
SHA-512:	C9B07FFC9758B50B4C201D3073056E47EC2208C0ADFEEE9B6458F235B1721EF233563D1C1EBDE50BC0C3BB550CAA28C713EB36FA273C96D622CC72439406CD E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/6332adb53a7e/RC0238d8e49fc8405f878b79a26e794e4c-source.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/6332adb53a7e/RC0238d8e49fc8405f878b79a26e794e4c-source.js`.._sa tellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/6332adb53a7e/RC0238d8e49fc8405f878b79a26e794e4c-source.min.js', "null! =window.wdgtagging&&null!=window.wdgtagging.oneds&&function(n,t,u,c){function a(n,t,e,a,i){try{var o=JSON.parse(c(\"input#cli_shellHeaderSearchInput\").attr(\"data- m\")),s={behavior:e,actionType:t,contentTags:{cN:a,srchq:c(\"input#cli_shellHeaderSearchInput\").val(),srchtype:i,id:o.id||\"\",sN:o.sN||\"\",aN:o.aN||\"\"}};c(n).is(\"a\")&&(s .contentTags.asdisplayed=!0,s.contentTags.resultselected=a),n=c(\"input#cli_shellHeaderSearchInput\")[0],ods.capturePageAction(n,s)}catch(r){u.debugLog(\"Error tagging microsoftstore links in the mousedown listener in the common tagging script. Error: \"+r)}}c(document).on(\"keyup\",\"input#cli_shellHeaderSearchInput\",function(n) {var t=n.which;13===t?a(this

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RC07c0b441f30340d784ae92a04518bb48-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):	23112
Entropy (8bit):	5.1265085892918645
Encrypted:	false
SSDEEP:	384:WHmvxF/hY1T2HnCW9duHw8HwYBiYDfneswTrdff:pvxF/hY1SHCW9IHpHwYnesk
MD5:	FD05BB028D6F7ED728FD889F472F9DBA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RC07c0b441f30340d784ae92a04518bb48-source.min[1].js	
SHA1:	9B232D4A5D405810951C6966D24E23DAA24BE551
SHA-256:	B0CDE14F235B95CFDD03A336DA7B4B6DDD51E6DE70E1DB0A6D06D55B17E7BB34
SHA-512:	BA05DD5B1600367048509E8A051DFF21A64E9E4167918C1D327619034CD86CA839A39E1FBAF59C7627C0E53CB5212ADE9B6437B8A19A36BF64F4714AB5FBE9C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/6332adb53a7e/RC07c0b441f30340d784ae92a04518bb48-source.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/6332adb53a7e/RC07c0b441f30340d784ae92a04518bb48-source.js`..._satellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/6332adb53a7e/RC07c0b441f30340d784ae92a04518bb48-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\0W10PBUV\RC0ee8c30f496b428a91d7f3289a2b8a2f-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):	1057
Entropy (8bit):	5.335017583671878
Encrypted:	false
SSDEEP:	24:D3m2lct/Bu3m2nU9lDMx93sHpQzb12Sjx5vRxVvRHy6IrBAuwuPn/:Dhat/BuhnB93sSb1PjxHx7Hy6cBbJ
MD5:	42F9F8885368EBFD43130F2D4AEEF5E8
SHA1:	13A44A4A62F5B079EAB4C7EBA3A264F13DD70C7C
SHA-256:	D8682829B8A56A003CA8EF1B28641F53AE2C087DA74D44C434A26EB3E19FE882
SHA-512:	D13FAC34768F32D653840ECEEB6B4883623DEA9D54E1C1BACFB2E0EB50297B4126DC668A25AC83F2FDE5319BA070B7333BBFE57B8CAD04760F4D0491C99F58E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/0f01b0e98be2/RC0ee8c30f496b428a91d7f3289a2b8a2f-source.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/0f01b0e98be2/RC0ee8c30f496b428a91d7f3289a2b8a2f-source.js`.._satellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/0f01b0e98be2/RC0ee8c30f496b428a91d7f3289a2b8a2f-source.min.js', "null!=window.wdgtagging&&null!=window.wdgtagging.jsll&&function(t,g,i){window.location.pathname.match(/\\en-us\\\\edge\\/?$/i)&&i(document).on(\"mousedown\",\".custom-overlay-table, .mse14-overlay-edgetable\",function(t){try{var a=i(this);if(a.attr({\"data-bi-name\":a.attr(\"class\"),\"data-module-id\":\"set\",\"data-bi-area\":\"body\",\"data-bi-id\":\"custom-overlay-table-close-background\"}),i(t.target).is(\".custom-table-wrap\")||i(t.target).parents(\".custom-table-wrap\").length||i(t.target).parents(\".custom-wrap\").length)return;var e=\"CL\";if(3===t.which||2===t.button)return;var n={actionType:e};awa.ct.capturePageAction(this,n)}catch(o){g.debugLog(\"Exp overlay tagging error: \"+o)}}}){wi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RC14999a828e04437b9286a3e42d5f4876-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):	517
Entropy (8bit):	5.347906365343886
Encrypted:	false
SSDEEP:	12:jvgefYpNBznfuct/BefYpNBznfTLgUl10aCKAnKofyKoAVZwuBB:DYTtuct/BuYTtYUl1NCVBfyBMZwuT
MD5:	81CCCE8C4F6C8CB68CE0E48BC24007E3
SHA1:	E4FFEFA721D7503587132D9E0C3D3B6A7758A7A3
SHA-256:	AF917C3132A69ED367C174FB19DA4DA0AF4808FC4400C22BB103F550F0A587C3
SHA-512:	923F85F05ECCD3428F37CA16D3A86BAFC6B46D3E97767DBF0B4FB11AF11F2A06F613F5091A7766BA46D0095D1A9DF2C8E7AF2078826D155B5341390025AF065(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/6b5c31f9d7fc/RC14999a828e04437b9286a3e42d5f4876-source.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/6b5c31f9d7fc/RC14999a828e04437b9286a3e42d5f4876-source.js`.._satellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/6b5c31f9d7fc/RC14999a828e04437b9286a3e42d5f4876-source.min.js', "null!=window.wdgtagging&&function(a,g){var t=function(){g.init(\"3j9k6rpcy1\")};a.category_all_status||a.category.analytics.status?t():a.category.analytics.queue.push(t)}(window.wdgtagging,window.wdgtagging.clarityTag);");

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RC15f7af7ffcd7475eaff80a9c2d39f0cf-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):	5802
Entropy (8bit):	5.349286114321429
Encrypted:	false
SSDEEP:	96:lBB4B6/kttzPHMKMWXFYq7AR4vW6LjfJy/PDjAKeKvtk+EPz/PGkbtD3K0tb1Edh:lB3kttjMKMWXFYq704vW6LjfJy/7EKeg
MD5:	F5D58FED023337F5B42EE6E7A50CA98A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RC15f7af7ffcd7475eaff80a9c2d39f0cf-source.min[1].js	
SHA1:	68E6867CC875055D0B0DD7A732FACD8C84F61840
SHA-256:	81D3644C44CFC966E56B67790F235DB0B1328131E25580C9DBB9C66471EBE319
SHA-512:	BC6FC550B82383D44C7DF97AF7A1432497AB4B7E420599342FB01AC002468852FABED1D7BD1383104B4DB4DA1A09CDE45BC9A910DFD620152DDCF8870A4A794
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/6332adb53a7e/RC15f7af7ffcd7475eaff80a9c2d39f0cf-source.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/6332adb53a7e/RC15f7af7ffcd7475eaff80a9c2d39f0cf-source.js`..._satellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/6332adb53a7e/RC15f7af7ffcd7475eaff80a9c2d39f0cf-source.min.js', "null!==window.wdgtagging&&null!==window.wdgtagging.oneds&&function(t,e,w,m){window.location.pathname;var f=window.location.href;w.wdgVideoTagging=!1,w.OneDSVideoTaggingInit=function(){w.wdgAttachedEvent={};var i=!(w.wdgVideoName={});m(window).on(\"message\",function(t){if(\"https://www.microsoft.com\"===t.originalEvent.origin&&\"Oneplayer iframe\"==t.originalEvent.source.name&&t.originalEvent.data){var e={};try{e=JSON.parse(t.originalEvent.data)}catch(n){e=!1}e&&e.eventName&&e.eventName.length&&\"Play\"==e.eventName&&m(\"iframe[id*=oneplayer]\").each(function(){var t=this;if(m(t).contents().find(\"video\").length){var e=m(t).contents().find(\"video\")[0],n=m(e).closest(\".c-video-player\").attr(\

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RC30b69654d14a4895ae64b6e5cf0cf812-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):	8055
Entropy (8bit):	5.304005982879021
Encrypted:	false
SSDEEP:	192:EBOutbhjqco07TGERdoXvL/XL5YxjikGeBf:EM6bhGco0fGEcD/XL5YxjiIBf
MD5:	CAA5BF7D582CD1E0890EB66C94CF300B
SHA1:	4A909837B76080E7D9C09D7481A4CCEF8087FE73
SHA-256:	EA9E163735E1E4429B0F530520BFC6492DCE4A4233B7426E260E4096F56ADC17
SHA-512:	579AF4F08187B3418BDAB475741834280967BEB19B74294B23FF6FAE2E6B674F2DF044DBD550D7E9B047452BD2D40722B8792FB6A1AB5D0EA676A7857A4D3980
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/6b5c31f9d7fc/RC30b69654d14a4895ae64b6e5cf0cf812-source.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/6b5c31f9d7fc/RC30b69654d14a4895ae64b6e5cf0cf812-source.js`..._satellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/6b5c31f9d7fc/RC30b69654d14a4895ae64b6e5cf0cf812-source.min.js', "location.pathname.match(/\\/windows\\/get-windows-10\\/?/gi)&&0<$(\"#mwf-hmc\").length&&null!=window.wdgtagging&&null!=window.wdgtagging.jsll&&(window.wdgtagging.data=window.wdgtagging.data||{},function(n,t,a,r,i){function e(t,e){i(t).attr({\"data-bi-scn\":\"hmc\",\"data-bi-fbid\":\"hmc\",\"data-bi-scnstp\":\"hmc-result\",\"data-bi-stpnum\":c.qseq.length+1,\"data-bi-field1\":\"fc:\"+e,\"data-bi-vtbm\":window.wdgtagging.data.sdata.vtbm+\";fc:\"+e,\"data-bi-sat\":\"fc:\"+e,\"data-bi-field2\":window.wdgtagging.data.sdata.vtbm+\";fc:\"+e})}jQuery(\"META[name='awa-pageType']\").length<1&&r.setMetaTag(\"awa-pageType\",\"HMC-page\"),(a=a||{}).sdata={};var c=a.sdata;c.qseq=[],c.qans={},c.current=0,a.ishm

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RC30bdc9ab3a2c421791b40b90f3faa2a7-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):	4176
Entropy (8bit):	5.239483229720829
Encrypted:	false
SSDEEP:	48:Dxt/Buc3Uqj7MrCs3N+azrHXxvbG8qkvddqGQNCoKx33/baoesXbu02w6J:9BBVwYaU678NTm//jLTfO
MD5:	DA2844C276A32231B83A2DF6FB40D291
SHA1:	BF4F404E805CC0A923E322FDAE77C3C10EBEB0C5
SHA-256:	0977C0D9F90172D70BECE96E4F0B20420FF47B133141A297DD3C0E932F54EB5C
SHA-512:	DC9D5BA4919424F51F9F6AF7A296F6790A7BF39DCFEC8600FD1E4A581EDD1DA0280185E8F3429D538FFD2C7837EE8F42468B5F9A722895DFE301582D107C23B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/6332adb53a7e/RC30bdc9ab3a2c421791b40b90f3faa2a7-source.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/6332adb53a7e/RC30bdc9ab3a2c421791b40b90f3faa2a7-source.js`..._satellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/6332adb53a7e/RC30bdc9ab3a2c421791b40b90f3faa2a7-source.min.js', "null!=window.wdgtagging&&null!=window.wdgtagging.jsll&&function(t,n,r){r(\".surface-clearfilters button\").on(\"mousedown\",function(){r(this).attr(\"data-bi-bhvr\",\"REMOVE\")}),r(\".c-checkbox input\").not(\".surface-hmc-ans-block INPUT\").each(function(){try{e=jQuery(this);var t=r(this).next(\"SPAN\").text();e.attr(\"data-bi-name\",n.tlcStr(t));var e=r(this),i=r(this).is(\":checked\")?\"APPLY\":\"REMOVE\";r(this).is(\":checkbox\")&&(i=r(this).is(\":checked\")?\"REMOVE\":\"APPLY\"),e.attr(\"data-bi-type\",\"option\"),r(this).attr(\"data-bi-bhvr\",i)}catch(a){n.debugLog(\"Error tagging name for Checkboxes section. Error: \"+a)}}),r(document).on(\"mouseenter\",\".c-choice-summary button\",functio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RC5d61fc978e53410f9823920e6f6ceece-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):	1286
Entropy (8bit):	5.27252138855126
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RC5d61fc978e53410f9823920e6f6ceece-source.min[1].js

SSDEEP:	24:DAfct/BuA7d+9SwTahWFR9fSZ8USZ8vSZ8DSZ8cSZzSZXSZ7SZhTKVwuGzS:D1t/BuOfJhWDtSnSGSGSjS1SBSlSTKVV
MD5:	1D5EE063D9D23A8B6CCFAFF3EBCDC372
SHA1:	12C8261570B92E59E97E7E63EE9B593FC4E9ABF8
SHA-256:	898CF373133D6394D27DDBF230BFDBCE75EBF5F35B0C09E50EE88E4A160C4AB9
SHA-512:	903AACA5F941596409214AE80E8453ACFFC1A66D7830B1FFF3B4C3BC2189A3E5007AF29A2D4CA5166D0E84DE71DB9E977159F1F13AE1414481B9B85DD071757
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/0f01b0e98be2/RC5d61fc978e53410f9823920e6f6ceece-source.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/0f01b0e98be2/RC5d61fc978e53410f9823920e6f6ceece-source.js`.._satellite.__ registerScript('https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/0f01b0e98be2/RC5d61fc978e53410f9823920e6f6ceece-source.min.js', "window.location .pathname.match(/\\Vedge\\Vuninstall\\/?/gi)&&null!=window.wdgtagging&&null!=window.wdgtagging.oneds&&(window.wdgtagging.data||{},functio n(n,a,t,e){e(document).on(\"mousedown\",\"#questionnarie button[name='btntellus']\",function(){var n=\"\",a=\"\";0<e(\"input[name='uninstall-reason0']:checked\").length&& (n=e(\"input[name='uninstall-reason0']:checked\").attr(\"data-bi-name\")||e(\"input[name='uninstall-reason0']:checked\").attr(\"aria-label\")||e(\"input[name='uninstall-r eason0']:checked\").val()),0<e(\"input[name='uninstall-reason1']:checked\").length&&(a=e(\"input[name='uninstall-reason1']:checked\").attr(\"data-bi-name\")||e(\"input[na me='uninstall-reason

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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):	5.333465569936735
Encrypted:	false
SSDEEP:	192:EB03+u1vwkOIOU574BraYQNRmDzB3Jf1bjZ6x8br8bWHcGdXG84HQMqhuG:EW+hkOI5791UDzB3JhjZ6x8br8bWHcG9
MD5:	CB2F4987C8D0F02FD6B63D162C4AC2B2
SHA1:	D247A2A1D99CB4AD1ED7E707F8363E4345B6D582
SHA-256:	88EECFF06842F9B1EEB50D4AFD2F25E0EBE5B9175377166EDFA4A60F21836D63
SHA-512:	0D9C563C52E369F78DD7D9F60C4994694481BAB3AF086E10B3223AFB111B10F2F1FEB0C9AB96CFA946B07358358226662E9FBE22222D42B1B3DE60080AA6852E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/6b5c31f9d7fc/RC5f812135e64f48ad85ea100034bc60a2-source.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/6b5c31f9d7fc/RC5f812135e64f48ad85ea100034bc60a2-source.js`.._satellite.__ registerScript('https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/6b5c31f9d7fc/RC5f812135e64f48ad85ea100034bc60a2-source.min.js', "null!==window.w dgtagging&&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.beha vior<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.vid nm,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=J SON.parse(a)).metadata&&a.metadata.video

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RC95d5954deda24aa780e2bd87a6eabf8f-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):	2996
Entropy (8bit):	5.3594637547654855
Encrypted:	false
SSDEEP:	48:D04Jt/Bu04kmTcmF8j4cELlGCnSwnDSRoSNiNcmF6RFuiWlW/04AvDR/YGH:gaBBXsLS5zi98RZWlW//EZ
MD5:	FE1E6451014A25BEDA4C79A513D3AFCD
SHA1:	74F843D058EBEFF8BB93FCC7DF1803FF82999546
SHA-256:	1D7E712DBEB20061E176A4008328610077D4C4D8756EFA091158EE58D46AE01B
SHA-512:	F22468E0075DF3CB03A7699CC413E8A003EC3DBA9BC970D37D4995D8BD2FCE5652FEA0F4098B52F10E576B6DC4A8446A87832431F6BC14EBB7B3367CAE835A 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/6b5c31f9d7fc/RC95d5954deda24aa780e2bd87a6eabf8f-source.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/6b5c31f9d7fc/RC95d5954deda24aa780e2bd87a6eabf8f-source.js`.._satellite.__ registerScript('https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/6b5c31f9d7fc/RC95d5954deda24aa780e2bd87a6eabf8f-source.min.js', "null!=window.wd gtagging&&null!=window.wdgtagging.facebook&&function(n,c,d,l){var e=function(){function e(t){var e=c.getProductInfo(t),n={content_name:r.content_name||\"\",cont ent_id:e.id||t.attr(\"data-bi-prodid\")||t.attr(\"data-bi-product\")||\"\",content_type:\"product\",lang_locale:r.lang_locale||\"\",partner:e.retailer||t.attr(\"data-bi-prtnm\"),cta:e.cta||j Query.trim(t.text())||t.attr(\"data-bi-name\")||\"\"};d.trackEvent(\"trackSingle\",d.globalpixelId,\"AddToCart\",n)}jQuery(\"meta[name='MscomContentLocale']\").attr(\"con tent\");d.globalpixelId=\"1770559986549030\",d.init(d.globalpixelId);var r={content_name:n.getData(\"gpn\")||\"\",market_name:n.getData(\"loc\")||\"\",lang_locale:n.getDa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RCa0f960a4cdc5494b98a97fc54841f54e-source.min[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\0W10PBUV\RCa0f960a4cdc5494b98a97fc54841f54e-source.min[1].js	
Size (bytes):	6479
Entropy (8bit):	5.32706988420496
Encrypted:	false
SSDEEP:	192:9Bl3+u1vwOPMR572qrP54vW6LjfIR/TtFoFDRcn0s/aK1Fhuc2R8X2TXLHsFSndx:9L+hOP67NLTMDRc09KXhu/R8GTbHW49B
MD5:	A9500BED30050CC1F00CDD63AEF25D9F
SHA1:	99C5B65B5865A7FEFEAE983CA4630ABB8D5EDB45
SHA-256:	97765F1AACD5B302246F833BA0EB79502C591896864AD3622662F8FF0C851A2B
SHA-512:	EB95E29C5D47C6559CA034C4261E1292A95EA9F59396142B0DFEB019B9A780212EA9231910595301ED6945CB3260F04A667A9E6FC2B09DF9F208210FC2D2669B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/0f01b0e98be2/RCa0f960a4cdc5494b98a97fc54841f54e-source.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/0f01b0e98be2/RCa0f960a4cdc5494b98a97fc54841f54e-source.js`.._satellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/0f01b0e98be2/RCa0f960a4cdc5494b98a97fc54841f54e-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,r=!1,c=f(\".c-video-player > .f-core-player\").find(\"video\");c.length&&c.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\0W10PBUV\RCaa8c2590551c47139847f13b302081cf-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):	1062
Entropy (8bit):	5.34344054774062
Encrypted:	false
SSDEEP:	24:DYGct/BuYgU9NMx93sHpQzb12Sjx5vRxVvRHy6IJBAuwuPn/:DYlt/BuYgL93sSb1PjxHx7Hy6yBbJ
MD5:	A373E321A805096735EF46269670B4AE
SHA1:	141F5FC6B0B319440F052D1AE1A42F0C841F60D6
SHA-256:	728E7C08421F769EF79B13728A92F21C3C40F1CA0FF745DD9F4355CFFE88D1BB
SHA-512:	35DA8FA314A15D1DD3F6805C3ADD8C8EF30D90139A38E34291C238EC4631BF250F7204A7192155947C258BED05D205B1CEFA03526ABD71CABF4F5AB7F4F168B5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/0f01b0e98be2/RCaa8c2590551c47139847f13b302081cf-source.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/0f01b0e98be2/RCaa8c2590551c47139847f13b302081cf-source.js`.._satellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/0f01b0e98be2/RCaa8c2590551c47139847f13b302081cf-source.min.js', "null!=window.wdgtagging&&null!=window.wdgtagging.oneds&&function(t,g,i){window.location.pathname.match(/\\/en-us\\/edge\\/?$/i)&&i(document).on(\"mousedown\",\".custom-overlay-table, .mse14-overlay-edgetable\",function(t){try{var a=i(this);if(a.attr({\"data-bi-name\":a.attr(\"class\"),\"data-module-id\":\"set\",\"data-bi-area\":\"body\",\"data-bi-id\":\"custom-overlay-table-close-background\"}),i(t.target).is(\".custom-table-wrap\")||i(t.target).parents(\".custom-table-wrap\").length||i(t.target).parents(\".custom-wrap\").length)return;var e=\"CL\";if(3===t.which||2===t.button)return;var n={actionType:e};window.ods.capturePageAction(this,n)}catch(o){g.debugLog(\"Exp overlay tagging error: \"+o)}}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RCbd62e4abe80c4cc5b3bcbaf6aaa28980-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):	5801
Entropy (8bit):	5.350724121781643
Encrypted:	false
SSDEEP:	96:gFBBXLB6/kttzPHMKMWXFYq7AR4vW6LjfJy/PDjAKeKvtk+EPz/PGkbtD3K0tb1w:GBMkttjMKMWXFYq704vW6LjfJy/7EKe6
MD5:	5418FE8C84CEC32A7A178A6CA26BCEEC
SHA1:	F2BC622E37115B32B58ECEABD735A10561D4B016
SHA-256:	5A68F395D4E2F2A19CB306115B7FD7B62580A04D103F7949CF4E783EAECC0792
SHA-512:	951F2D283ED6AB163B46CF9EB2FD1406562C05DE0AD459D57C3C3340805C0A498CCF6920D79BDA383FB8F1BFDD64CF823DC1578642FB06E7179087BDA95CF52
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/6b5c31f9d7fc/RCbd62e4abe80c4cc5b3bcbaf6aaa28980-source.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/6b5c31f9d7fc/RCbd62e4abe80c4cc5b3bcbaf6aaa28980-source.js`.._satellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/6b5c31f9d7fc/RCbd62e4abe80c4cc5b3bcbaf6aaa28980-source.min.js', "null!==window.wdgtagging&&null!==window.wdgtagging.oneds&&function(t,e,w,m){window.location.pathname;var f=window.location.href;w.wdgVideoTagging=!1,w.OneDSVideoTaggingInit=function(){w.wdgAttachedEvent={};var i=!(w.wdgVideoName={});m(window).on(\"message\",function(t){if(\"https://www.microsoft.com\"===t.originalEvent.origin&&\"Oneplayer iframe\"==t.originalEvent.source.name&&t.originalEvent.data){var e={};try{e=JSON.parse(t.originalEvent.data)}catch(n){e=!1}e&&e.eventName&&e.eventName.length&&\"Play\"==e.eventName&&m(\"iframe[id*=oneplayer]\").each(function(){var t=this;if(m(t).contents().find(\"video\").length){var e=m(t).contents().find(\"video\")[0],n=m(e).closest(\".c-video-player\").attr(\

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RCbdb0f3827f8d43f3a1e00247bf63d9e4-source.min[1].js</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>ASCII text, with very long lines</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>1032</td></tr>
<tr><td>Entropy (8bit):</td><td>5.296025977831885</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>24:DQsct/BuQqU9lHJ7UOzSE/xFAChIKu8C1ijkiJi0i+DDnAkwuKIPn/:Dwt/Bux6+VE/TjLCCrDMkr</td></tr>
<tr><td>MD5:</td><td>32844B0CBDBC49C212F30F0D30DD8F9C</td></tr>
<tr><td>SHA1:</td><td>0CD9C10F9845C0942B4AA2B5702CA07E475502C3</td></tr>
<tr><td>SHA-256:</td><td>CEED0C8C90072E9E4D19AC0C37556C1D3FDF40B8D028C497586A13D07484E3D9</td></tr>
<tr><td>SHA-512:</td><td>F67F03D05D70EDE609B528DC78BCB1566EF55C623E9A9E90CC4067C54163FF91EFE328775473E481015F37A03D78E6F78CDAB1CFF299353C927CCEDB88564C2</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/0f01b0e98be2/RCbdb0f3827f8d43f3a1e00247bf63d9e4-source.min.js</td></tr>
<tr><td>Preview:</td><td>// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/0f01b0e98be2/RCbdb0f3827f8d43f3a1e00247bf63d9e4-source.js`.._satellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/0f01b0e98be2/RCbdb0f3827f8d43f3a1e00247bf63d9e4-source.min.js', "null!=window.wdgtagging&&null!=window.wdgtagging.jsll&&function(a,e,t){var g,n,i=_satellite.getVar(\"CurrentSiteData\");location.hostname,location.pathname;if(i&&i!=undefined){var w={appId:i.appid,version:\"4\",coreData:{env:a.getData(\"env\"),market:a.getData(\"langLoc\"),pageName:a.getData(\"gpn\"),pageType:a.getData(\"pageType\")}};w.prePageView=(g=a,n=t,function(){n.setMetaTag(\"awa-env\",g.getData(\"env\")),n.setMetaTag(\"awa-market\",g.getData(\"langLoc\")),n.setMetaTag(\"awa-pageName\",g.getData(\"gpn\")),n.setMetaTag(\"awa-pageType\",g.getData(\"pageType\")),n.setMetaTag(\"awa-ver\",\"ccStatus:\"+g.getCookieStatusInsights())}),e.load(w)}}(window.wdgtagging,window.wdgtagging.jsll,window.wd</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RCd01d50cad19649bf857a22be5995480e-source.min[1].js</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>ASCII text, with very long lines</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>1070</td></tr>
<tr><td>Entropy (8bit):</td><td>5.369300956154228</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>24:DqQMct/BuqQKbEfgwiUtB7eOE7ZewCEArRWxGJiwuPn:DqQ7t/BuqQK6gwiMB7lE7YKArwxeidn</td></tr>
<tr><td>MD5:</td><td>D9FCED2FA0B90FB40E78522ADADF205D</td></tr>
<tr><td>SHA1:</td><td>464FF964FED2BA37E7787D5348CBC8FA991DC4BB</td></tr>
<tr><td>SHA-256:</td><td>21CA186214D481A75F7CCB0ED5D44871D7BE8A0F68A8780FB2DCB6E4F98E31FB</td></tr>
<tr><td>SHA-512:</td><td>EC7617E94CAF62CB8ED3C28FBE9580BC8103AD079EEC598BA8C08560906E8B0515822647065413707265 33A4827450E903F9D83FC2A58BF463718E79C789E13C</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/0f01b0e98be2/RCd01d50cad19649bf857a22be5995480e-source.min.js</td></tr>
<tr><td>Preview:</td><td>// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/0f01b0e98be2/RCd01d50cad19649bf857a22be5995480e-source.js`.._satellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/0f01b0e98be2/RCd01d50cad19649bf857a22be5995480e-source.min.js', "null!==window.wdgtagging&&function(t){var a,o,e,n;(0,window.jQuery)(\".at-flicker-control\").slice(1).remove();var i=location.hostname;location.pathname;a=i.match(/^(www.)?microsoft.com/)?\"prod\":\"staging\",(o=window.location.pathname.toLowerCase().split(\"/\")[1])?o.match(/^..-.*-..$/)?(e=o.split(\"-\")[0],n=o.split(\"-\")[2]):o.match(/^..-.*$/)?(e=o.split(\"-\")[0],n=o.split(\"-\")[1]):n=e=\"\":n=e=\"\";var g=window.location.pathname.toString().replace(/^\/(.*)/i,\"$1\").replace(/\/+$/,\"\").toLowerCase();(g.match(/^$/)||\"true\"===document.getElementsByTagName(\"body\")[0].dataset.homepage)&&(g=\"home\"),t.setData(\"env\",a),t.setData(\"langLoc\",o),t.setData(\"lang\",e),t.setData(\"loc\",</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RE4hgqN[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 359x234, frames 3</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>4679</td></tr>
<tr><td>Entropy (8bit):</td><td>6.371893948874056</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>48:QffuETAf3NW6aLZ0r0dd3DZAUL0qPx9xj3aWH5IDoy:Qf2EwNsL6rwTZAPq1OCSoy</td></tr>
<tr><td>MD5:</td><td>0C62F2E3C52BF24EE50D29EB3A077172</td></tr>
<tr><td>SHA1:</td><td>9D314F7ED5F3C22806CBD15AF67641856AADA01A</td></tr>
<tr><td>SHA-256:</td><td>E4BD64DF2AC8A577F9D2BF27BD32B880E6DA8A6BDE751C7BC9F6E0DEC373F68C</td></tr>
<tr><td>SHA-512:</td><td>E94C89E26B226FFA8CB9CFD204FF5DEA74376DA0D21460C1A043BB090F61DB1D6A7A48FBF206DB70CA5C5A47543E052DF74D2374B6DA3D39F78BFE54C05F2D
73</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>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</td></tr>
<tr><td>Preview:</td><td>......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO........g..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?....(......(......(......(......(......(......(......(......(......(......(......(......(......(......(......(.k{K...ko4..4-........q...=~....@.g....\C$M..R...........(......(......(......(......(......(......(......(......(.........u/.\..b.J.y;....>.=[C.y..j.u....W.|..'O.4...j.f.l.vH..,Q.....a...Iyv<7....5..f.]CH.1...1.E"....$...[....I........:.....v.?*d.U.h...zmu..m.Xr.=T.....</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RWBtR2[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:	downloaded
Size (bytes):	67715
Entropy (8bit):	5.426751829904342
Encrypted:	false
SSDEEP:	1536:wHmIRJJ9Zm4nzKF5ZH/KhoLGYhz3jEj9TNfHx7EmI9oNAzBbX:wlRNLU0Y7d
MD5:	55CE123F12E597046725CB0A40E8E4BA
SHA1:	87C57E93E78B77AC3EEF7B074A0B8DC3574A0153
SHA-256:	AC06F4CB38651F4A269C97F686125BF01C6042441F46A75895DBD70A824FA39A
SHA-512:	8D655FCD868BE9ACF8929362506D26E9E7AAEDB4E53229353F055351285F43FEE5A4FC27D3F0F998621685BE88EA50F0228C35E070C8C9A2C58E1F7AFFE1E8E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/en-us/videoplayer/embed/RWBtR2?pid=player-container1-oneplayer&jsapi=true&postJsllMsg=true&autoplay=false&mute=false&loop=false&market=en-us&useAdaptive=false&playFullScreen=false
Preview:	.....<!DOCTYPE html>..<html lang="en-us" dir="ltr">..<head data-info="{"v":"1.0.7823.38521","a":"208e62d9-b47c-48b5-aba6-a59e5ed91132","cn":"OneDeployContainer","az":"{did:92e7dc58ca2143cfb2c818b047cc5cd1, rid: OneDeployContainer, sn: marketingsites-prod-odnortheurope, dt: 2018-05-03T20:14:23.4188992Z, bt: 2021-06-03T05:24:02.0000000Z}","ddpi":"1","dpio":"","dpi":"1","dg":"uplevel.web.pc.ie","th":"default","m":"en-us","l":"en-us","mu":"en-us","rp":"/en-us/videoplayer/embed/RWBtR2","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></title>.. ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RWF2OQ[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, baseline, precision 8, 320x96, frames 3
Category:	downloaded
Size (bytes):	13643
Entropy (8bit):	7.968254408184841
Encrypted:	false
SSDEEP:	384:nGCC3cQ9Pb/I8k3Igh/bn+eH5Usqlkf1BnBLY:dCsQhA8m/bnbH58lg3Y
MD5:	9DF1D92C0E57571D7351ED5D5D01D716
SHA1:	6F442A8D626AAB245FE4F75C9520CA627D97FD56
SHA-256:	D438F4BA9B21C43BE5B4B1E9AB71D8C52CBDC1E6B38A60E3DB8F8A59EFFA2A0E
SHA-512:	A956215A159812F9E3DFEAD6CBE873250329FDA7DE0CBE146A8366AB05BACA7B6F4D542B3F9910CF0C62EC2742B41C04BB0AAC7E0CA763A15FCD8EF987E78 28
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RWF2OQ
Preview:	.....(....Adobe.d.....`.@..... .!1.A..Q..aq.."....2...#3B...$b..%CR.45DEs.....!...1Aa.Qq...."2....3r.#$BSb.....%CR..&'4Ddeu.Ucs.....?...J.$..Z....0...l.{..v.%...sN..T.2.l....$#.BE.;...g. eA.@. <...r.`.N.*T...\?3....ta...1.....+r.l.{l.$...e.o9%.K.D.... wBx..Ns{..W#..C.g..!t%D.z4jh..N<s.bDD`<...._...t..<c....%...9$.5.Y.o.o]...)IC>v.M.....3....bvQ.(g....d.P..C..<Y.D.. .P..w]5.. 2.....G.&...$..n\.k.|..A....YS..N..(,.....8..._)..xb..{.,).d .j..LrY..d...._.6.....5ee.I.:.....l.c...9&.c.@~.X...W.~.;..l...=v>.q. 4.....!fT.{8?=.....f..v...S:....B.C].w7.*.q.....O.%./... {1..8....GE.cs..%.jZQ*S.{.n.....<...4e....r...J.....s1.../.dWu....%.1...=.....Q,y.Z...?.#t..4....[...\....~s.W..H...N

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Home_HMC_HighlightFeature_Spring_21_V1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 1920x720, frames 3
Category:	downloaded
Size (bytes):	101119
Entropy (8bit):	7.288488281826517
Encrypted:	false
SSDEEP:	1536:BXk+j0dXdFalFSUe1RR8zlK/OJuQwbfz2/ySGmvXW1ewJk/rjkAbrf5jSRhDM9/i:BXviXWe98cpJC/y2Se0k/EA32hDt
MD5:	FA77084E64AF11C74A68CF4B84679FEE
SHA1:	EC512C03E1BA977D751CC27C4C27F4D2A93ECB19
SHA-256:	BF8CB95D39A5B278D5ADB16191876A24D0CCB618BD6A9D00ACB687806699F9B9
SHA-512:	BAD344850533E823F6B4520CB56237DA307F4D4B1CFF7BCA89AD63ED1AE749FD4642F4F73E7DAF741ACBA401C686AB0A128F7D7ED91252FCD549CC9A728EC D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Surface_Home_HMC_HighlightFeature_Spring_21_V1.jpg?version=03ed24a9-1ad2-b0e4-effb-c43b598c1d54

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Home_HMC_HighlightFeature_Spring_21_V1[1].jpg	
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 6.0-c006 79.164753, 2021/02/15-11:52:13 "> <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:16C0076A85F911EB9AD38DD4886F9E49" xmpMM:InstanceID="xmp.iid:16C0076985F911EB9AD38DD4886F9E49" xmp:CreatorTool="Adobe Photoshop 2021 Macintosh"> <xmpMM:DerivedFrom stRef:instanceID="D1A0B248B22ACA2B39FC9616411AFBA1" stRef:documentID="D1A0B248B22ACA2B39FC9616411AFBA1"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Home_Hero_20_mosaic_Book3_SingleTile_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):	58053
Entropy (8bit):	7.533535899344126
Encrypted:	false
SSDEEP:	1536:jHDpL9XyoEM9oVf+FD5PPQ0RYukdpJoAr2TAr:TDp8HYoVfgA0ap/2Ti
MD5:	EB0EAC625C2D1D8393985978AD929786
SHA1:	097AFA66C015526F9EE47C197F55126F1E780B9E
SHA-256:	520B0AFDED6D818CD7A8AC6BC99A7BEB3BB55711CA79196C8BD48F7112D6DAE5
SHA-512:	C64E19C3E00FB7368FD873B1BF7E7DB9872995070FC40239601F668FFBE992AB749A492B2EA1ABDF500ABF6E44BCA8F1407DCD143FC6B5CF756502086D6E4DA4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Surface_Home_Hero_20_mosaic_Book3_SingleTile_V2.jpg?version=8f322e33-582d-30a2-ffaa-4ce4b60775e4
Preview:	......JFIF.....+.....]..... J,.....M&.G..h.....S.....x..].5..>.U....j.6.Z.f../;{{d.....~y.E.v..f..|+...E.6mY....^.....t[.n.V.[.f.{T\..... .....Q.?.9...r2.rr....s.s2.U.....8....._....QM4.....'..Z.....3@.....TQE..M4.D .x#.....>...h.)."..~<.+.....K...(..i..b"".Q.~.....t.sQE.QM4.....(xo.=.X.....>....QE..M4.1.....>...d.....h..i..b""....Lx..(.....h..).....>....{0.....<w..*i..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Home_Hero_Spring_21_color_V3[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):	60618
Entropy (8bit):	7.944701815502637
Encrypted:	false
SSDEEP:	1536:ccULmd9c9+kGx4WRYhxghX8znL2Nbbvg0Ga0hKP:zULEWAfxxYhkXyKNbbvRGa0hKP
MD5:	135797F37B8303ACF014E4EDAFE17CCC
SHA1:	BFA783BAF387ABC4DCF7CC1019B96F953B3B1DEC
SHA-256:	47B18E2B672836385486B1C15F92B4BE9EA389EF84287C1FE3B10D0A1AEC551B
SHA-512:	F50F11BF8AFFBC20F00C4C1F632587FB92CD0CCBAF648B241A9ECE2A7842D764431E82EA0748CACC25A193B0173C852B5676AE53B8D4661B4A933A839A9E2B5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Surface_Home_Hero_Spring_21_color_V3.jpg?version=61644a07-e383-9dd6-69af-feb8ab6a52e1
Preview:	......JFIF.....a.;.....UT(.....P .....r..*..C.$.X.$.a1.$...a&..I.j.....$.2..i....T.|3.}%.HLb.$.L$.L$.I...$.a.....Z.*"..****..(E.....`...[m{...H./.>i..%...D1..$...I0.I0..0.L$.}.*"*.***"..**.*...@.b..D.WG.m.c....>k....r....q]u..$...I...I..L&.a...U.Q.Q.QQ..U...U.UP....,.L.6tt=.=.=.;F.?.....UUH..,I$.a&.a&.L0....!>..Q..QQ.QkUDUET...@..P..W...^.I.....~r..._a....3f..5UMu"...L$.a$.a$.a0.a..=."*-j....QU.QUU@.@Q.#"tvX..e.u.Yk...s.W....._..s.Zj....+TU..L$...0....!&.=.*".**.****..**...b@..Nm..{...;'K...|g.K.....^..~O.g.+.....@..L&..0.....DTEDUDEEDUEETUEU@.@..W%....,..p.....o...c.\...._j....i..j.VC.C.&.....0.a.{.TEEDTEDUDTUEE...(P.....,..8..A..>g.O.]....K.}/.....~.EUDJ...s.E4.....0.I..$$..&{.EDTTTEDTTTTUETUUU...*...]y\,.d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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//wtIMq
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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Home_Mosic_Fall_20_Duo_en-us_V2[1].png	
Preview:	......JFIF.....+..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Home_Pride_5_21_V1[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, 1920x720, frames 3
Category:	downloaded
Size (bytes):	478551
Entropy (8bit):	7.977185080604146
Encrypted:	false
SSDEEP:	12288:sFEF4H2209aerMOmP1J2iWrgcPUbUu+p2:s+F4HdVeAXbjWUcMTU2
MD5:	2A994B50D4755DE364798ECF3EAEAD26
SHA1:	B85AFAA456356E8C3AD3ADD483BA875341A91127
SHA-256:	69A8F4751C6C32C77706BDF158C0D33A7CF6F163A2D708DBF19D17AE19F634B1
SHA-512:	0D92289141C388C703EAA958AA270122B90DAE7D39951F7B0925FB80EA5E2671F52E4EBCCD55DA41DBD30F47E2BF7D6C8A2E5AFBF7F689EEAB4286A55AB714A3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Surface_Home_Pride_5_21_V1.jpg?version=476ede35-ac58-7627-54d1-fac8eecd64a4
Preview:	......JFIF.....P.....~/Q.c....+.q c2.i...1.e.i.IVs.b..QU...5...>5S.X..W.h.....C3.*.UvBP.8.G.N5.3...ds.Ueu'euB..1.f.+..Y.e^*.~.....~/R.fU\!.Q.1W.s....:s...+.1....<U...U+1...5...gI..... ..+..t...v.4..',..x1.B.F.UM..I.Zv....#..8.v.F.J...H.....?....:}<i...*..1(.....a...b.KM..8WdPa.....0.....8....1*..QTk....0.3+j.M.c8.4k..Vb....c.YM1.T.(':.f0.~..... .....Z...g.h.).a....9Y....W.b.q.Uf%,.j3.....b.>3+!..Vr..}.....q...!R..Fi.!..1....N..GO.C2.IE<..Q.g.l.y...b6bh.2.....Ru..B1.....g.....l!....c..8.Y...]r...(.q,.1n1,..3 .h..p.....8.....jqJ....0BTg1...#...Uf.G3.f!...".6i.k.!.%L.,cK.a.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Lg_Generic_ContentPlacement_3UP_20_Acc_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, 321x180, frames 3
Category:	downloaded
Size (bytes):	15307
Entropy (8bit):	7.945889383716535
Encrypted:	false
SSDEEP:	384:fMJJf2IBFNTk0IKBWaok20bL3Yvcdkin3jOSMZ:UByOWJkBscvbi
MD5:	952E81EAD4DFAE967BCDAF662DBBC9C2
SHA1:	09E9290D7F76CF4D801212DE8AAE1C5141913665
SHA-256:	3C17D996C66C3714676E2061BF6E437E6F6D5C79A396B350D3ECC0BD2945A4E7
SHA-512:	7DC2175B317A65E0988A25BC8B16CC8E4CD1E10218E7C3D2C73BF665BEEFD074D87A0E39D74FC0CFC468F79FC31FAC6286D8F02B2728C20668E974654B474AB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Surface_Lg_Generic_ContentPlacement_3UP_20_Acc_V2.jpg?version=4df8358b-48ad-3cd0-3727-4d09acaeae79
Preview:	......JFIF.....A.....x.4I%B..F..9U7..q..V...5\.&r..r.& .h..U|.....]mT...U.-.|iZ.U'.8.U/.vV.n...H.j...h>...Ml.....1...B....u@..h..5.{A..[c..x..B...mu8..r.....i..qS..?.-..1.....(z7.T..G.9..`..G..5|..X..yLS2....h.....Z.....r._.....#.d.,K.B....y..... $]....X.?...+.....m.....37.>..<..U....o.....S..K.....`.;....h.k..>.....K.c0.+&..a...bA\z~..6...u)C..C..Ag.#...;F...9..^R...<.K.o.....z.7 ....yI....mE..2.Er.v...x.....T.I..69M?Y.P....My. .....h....z...Z....|<..6..)h...iQC...+cUR..!.=.vU.....y.....yd?..2..JW``.yg.A.<..s*.....5H.....6V.0...t...;.'49.g.. ..[H..,uV.....V....f..sc.....3.tM...Mu.....Q....U.....y.....I[m^.p;....._:N. .&..l..5.n.5..V...fq..s94..K.O]...9..0C.^cv=g8..;.N.4...j.$\....@.m...7..V.....W,.....@.....0.3:..=.4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Lg_Generic_ContentPlacement_3UP_20_Business_V2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 321x180, frames 3
Category:	downloaded
Size (bytes):	22129
Entropy (8bit):	7.965327363975181
Encrypted:	false
SSDEEP:	384:rAA7g0vjdZPa8O2LJ+nHi04WDbZdhaHnln090bomH1BkQvsSgYOoLGpXx:rAAdZPz9Jz04WZYnOmdpOoLGpB
MD5:	C766D24566658FAB6CC360AE0059B822
SHA1:	7AF74159F2CED01FEB9C231DE122BEBC71B3EF54
SHA-256:	3AEB1CFF75E02A1D197AE7E2CF269A0200D0D92539FF4ECD14F4502A8B7DB9B0
SHA-512:	4A34160F728752A21DF42B6E5323FEC17B091D62DA5894B1411D7248CB9BE482BEAB3444212B0F77BFEEB1886670B74D9589A1E8BB20CEB31E8C9FA679523D0E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Surface_Lg_Generic_ContentPlacement_3UP_20_Business_V2.jpg?version=4f2896bd-0349-796d-e115-cc617291dce4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Lg_Generic_ContentPlacement_3UP_20_Business_V2[1].jpg	
Preview:	......Exif..II*.....Ducky.....P.....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:7E6E3AA8917511EA96B8F13B1A010E1A" xmpMM:InstanceID="xmp.iid:7E6E3AA7917511EA96B8F13B1A010E1A" xmp:CreatorTool="Adobe Photoshop 2020 Macintosh"> <xmpMM:DerivedFrom stRef:instanceID="A3345D466467131E4C37D35A8DE426A4" stRef:documentID="A3345D466467131E4C37D35A8DE426A4"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Windows_Cortana_AppStore_img[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop CS6 Windows, datetime=2017-05-08T13:01+05:30], baseline, precision 8, 303x90, frames 3
Category:	downloaded
Size (bytes):	14984
Entropy (8bit):	7.909338786513498
Encrypted:	false
SSDEEP:	384:TUnEMF/izFabOzR4Nz+EhoRNLqm2EHDNU66k:TUEKicOzEhoX35Z6k
MD5:	C843BD8FE087CF834754FA771881AA18
SHA1:	B6DA0FB9D8AFD593358520738E7F3C955461F3E8
SHA-256:	B5D49AC945648AB0CB3D40460DE1F57A8EE51609AA4CFCFE2E973F278B6C9D44
SHA-512:	95BED5B70816961ED923EA55A84DC28B7334657E5FC769DA2FB81D668A9992A0E5C982770742940BB3F6893707DFDE9F4EE81F22C1912BB6FA50A32DA06299F8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Windows_Cortana_AppStore_img.jpg?version=b435fb28-7075-160f-377a-1fdf1160e2dd
Preview:	......Exif..II*.....b.....j...(.....1.....r...2.....i.....`.....`.....Adobe Photoshop CS6 Windows.2017-05-08T13:01+05:30.....0220...../.....Z.....Z.....Ducky.....d.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <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:dc="http://purl.org/dc/elements/1.1/" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:48E74BC833C011E794658E8F355BFA24" xmpMM:InstanceID="xmp.iid:48E74BC733C011E794658E8F355BFA24" dc:format="image/jpeg" xmp:CreateDate="2017-05-08T12:55:25+05:30" xmp:ModifyDate="2017-05-08T13:01+05:30" xmp:MetadataDate="2017-05-08T13:01+05:30" xm

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\agavedefaulticon96x96[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 96 x 96, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1115
Entropy (8bit):	7.474905425501729
Encrypted:	false
SSDEEP:	24:OQkGe2gKOcQO9S80Axzhkzc7iFTZkqeNblj5IlIN0EFgFahPKN7FqP8:OQkRrTCbxzwSiZLCN52TFgM5KN7Fp
MD5:	084E7612635DFCF69A16255B41E70CAA
SHA1:	0D9721AA70B01487D3340B864C0BD49FB1D95206
SHA-256:	7B389747818635BCA6FE76F5E3226EDA36AF53D8F27526796BC975EBD440A395
SHA-512:	A0104DBB40429BCA5F54061CE6D36A695283D883CE1B732CA87A30743234D29BEBA07A0100DE0DE0B274A70C8C7C289574F6343DF16C3E4C7B6453F60E8737B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c1-onenote-15.cdn.office.net/o/s/161411141024_resources/1033/agavedefaulticon96x96.png
Preview:	.PNG.....IHDR...`...`.....w8....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^.k.A.....@ .6.* ..H...R....V....l.! X..Z..Z..... X... .. .{.^fw...{.fv..70.~..|..... .. ..3.8.1q....(.&.....B.o..''w..Y.....]......~0N0....]..z....|.n.*.....,_..O...9..8@..K./..%..[..LQ.rm:.H.>...-..;,...9.G.n....`.{..-.F...'.?...y..]H..o{y..#.....]..x|...K.(x|p~.....r..R..~\.2.Y...f.Q..i...o...r.....Gc..Bp.Ol..\(...~.T..,....j.O.(e.....j(e. ...Z....Rf.....j(e. ...Z....Rf.....j(e.....D.,Y.....~..n.[.....PA....]....0.mK...sE.....J~}z[.!n...RV|.#.....7s.....)B.e;j2.....tX..k.....o.V....j.k3*A.....9..?R....Z....5t..j....f.Z.....E.L....J..7.}Uk.....H..i.Z...1...x$....]<I.....#ixw..h.h.h.a.4....9.&.v.....2i..D..I...'.-.+.._...eLZ...M..x..1%.g....'A..X.....jkK.^W.}.m...T....|....._^.[..~u'...mco.8...nT....d.m.I.b..M.4...s.U.;Yu...k.1|..93a..(M..2..U.....B..S..O.....c.....?)....iz.D...T.D!....R

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ai.0[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	96705
Entropy (8bit):	5.228470338380378
Encrypted:	false
SSDEEP:	1536:EVpXOWPGHRGUvJEzxPNLgyLuG6XV3yV/QtJ+j1YeO4PFWYit:EVoWPGHRGUvJEzxOMQV3yV/ERaNWYit
MD5:	1DD63DE72CF1F702324245441844BE13
SHA1:	58A8BDCDCB398AF7DB424357DF70DF18E7B30E9D
SHA-256:	5201C813C37A4168CC5C20C701D4391FD0A55625F97EB9F263A74FB52B52FD0E
SHA-512:	532D1E907B433AB97785CF632D9637A957152BAF0BA57879C856CBAA469BFFECA22C4F99485679539944B27068D39E70F7D44282594F999142454DA57329A11B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ai.0[1].js	
IE Cache URL:	http://https://az416426.vo.msecnd.net/scripts/a/ai.0.js
Preview:	"use strict";var AI,Microsoft,__extends=this&&this.__extends||function(){var i=Object.setPrototypeOf||{__proto__:[]}instanceof Array&&function(e,t){e.__proto__=t}||functi on(e,t){for(var n in t)t.hasOwnProperty(n)&&(e[n]=t[n])};return function(e,t){function n(){this.constructor=e}i(e,t),e.prototype=null===t?Object.create(t):(n.prototype=t. prototype,new n)}}();function _endsWith(e,t){var n=e.length,i=n-t.length;return e.substring(0<=i?i:0,n)===t}!function(e){e.ApplicationInsights||(e.ApplicationInsights={})} (Microsoft||(Microsoft={})),function(e){var t;t=function n(){},(e.Telemetry||(e.Telemetry={})).Base=t}(Microsoft||(Microsoft={})),function(e){var t;t=function n(){this.ver=1,this. sampleRate=100,this.tags={}},(e.Telemetry||(e.Telemetry={})).Envelope=t}(Microsoft||(Microsoft={})),function(e){var t;(t=e.ApplicationInsights||(e.ApplicationInsights={})).Context||(t.Context={})}(Microsoft||(Microsoft={})),function(e){var t;(t=e.ApplicationInsights||(e.ApplicationInsights={})).Context||(t.Co

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\app[1].css	
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):	262641
Entropy (8bit):	4.9463902181496096
Encrypted:	false
SSDEEP:	3072:u+Vd0pBbqPLYoyjFkxD2hAYwJb8ILm731Ss:u+Vd0DePLYoyjFkxD2hAYwJbZLM31Ss
MD5:	7C593B06759DB6D01614729D206738D6
SHA1:	0D4F76D10944933B8DDECFFE9691081439A77A3C
SHA-256:	F7D9FB0479DE843CF3FB0B78FC56BBB9E30BF0A238C6F79D9209FA8B22EFB574
SHA-512:	EF91B610CF17A17AAFB48984B4403EF175EB86096E3F12E23AE8D4C7C96EF60ED14DA3F69721E095CD2ACE3F0A06190186D000992823814BB906F7FB3576C2C1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.onestore.ms/cdnfiles/external/oneui/oneui1.16.2/dist/css/app.css
Preview:	@font-face {. font-family: "wf_segoe-ui_normal";. src: url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot");. src: url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot?#iefix") format("embedded-opentype"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.woff") format("woff"), url("//i.s -microsoft.com/fonts/segoe-ui/west-european/normal/latest.ttf") format("truetype"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.svg#web") format(" svg");. font-weight: normal;. font-style: normal; }..@font-face {. font-family: "wf_segoe-ui_light";. src: url("//i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.eo t");. src: url("//i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.eot?#iefix") format("embedded-opentype"), url("//i.s-microsoft.com/fonts/segoe-ui/west-euro pean/light/latest.woff") format("woff"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.ttf") format("truetype

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bullet[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKIv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/bullet.png
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:...a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\c9-860587[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):	329706
Entropy (8bit):	5.296682106283116
Encrypted:	false
SSDEEP:	6144:xAuXzUqR1s9g0qRORPvksdmXc73pCq9a22j:xvzUBg4za
MD5:	B508477CF2A68E45669C7827315872D8
SHA1:	35002085580EA4288CE81B9F0417C3E3AB166DD5
SHA-256:	525A139B66C6F666AE81FCEE16E56EF7AEFDAF5F41E951C210186B2E09317F09
SHA-512:	3E1E5DABD53D185673E44E84C8B445629F9924FFEE81474636F4601FBA3506994641DB68BD6D42B2AA948F32D02E9167A44922EDDF026FFFF8BCCF976DF9BE7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\c9-860587[1].js	
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/mscomhp/_scrf/js/themes=default/e1-a50eee/e7-954872/77-04a268/11-240c7b/5c-0bb0c0/81-a5a694/2f-63ce8f/6a-f6eed8/dc-7e9864/4f-5115f8/7d-266f10/4a-abd94b/ab-b04110/fd-7cc407/a4-fd2a9b/7b-131f20/66-c19a96/d0-633018/74-b70f5f/84-e0fd46/cb-abee28/1d-c29f1e/80-c05e42/a5-ef9ca1/f8-6a3735/b8-96db64/b4-d9c6d1/59-aa2448/d5-2b21b0/c5-346220/d6-6bf74f/d8-e94c5c/b8-527d75/57-0776c0/7a-fdafe7/18-91dd3c/88-3094ff/bf-4fabe5/f3-89463b/12-fd63db/85-b1c94b/6a-582442/64-02965a/37-f22d3d/33-eb67f7/fb-890cea/c9-860587?ver=2.0&_cf=20210415
Preview:	define("componentFactory",["require","exports","htmlExtensions","utility","stringExtensions"],function(n,t,i,r,u){"use strict";Object.defineProperty(t,"__esModule",{value :!0});var f=function(){function n(){}return n.create=function(t){for(var i,r=0,u=t;r<u.length;r++){if(i=u[r],!i.c&&!i.component)throw"factoryInput should has either component or c to tell the factory what component to create.Eg.ComponentFactory.create([{ c: Carousel] or ComponentFactory.create([component: Carousel])";n.createComponent(i.component||i.c,i)}},n.createComponent=function(t,r){if(t){var o=r&&r.eventToBind?r.eventToBind:"",f=r&&r.selector?r.selector:t.selector,s=r&&r.context?r.context:null,u=[],e=function(n,f,e){var a,c,l,o,h;for(a=r.elements?r.elements:f?i.selectElementsT(f,s):[document.body],c=0,l=a;c<l.length;c++)o=l[c],o.mwfInstances||(o.mwfInstances={}),o.mwfInstances[n]?u.push(o.mwfInstances[n]):(h=new t(o,e),(!h.isObserving||h.isObserving())&&(o.mwfInstances[n]=h,u.push(h))))};switch(o){case"DOMContent

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\c[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	42
Entropy (8bit):	3.0241026136709444
Encrypted:	false
SSDEEP:	3:CUXPQEsJ+q:1QEsJ+q
MD5:	32023BB33CFB2A1990A4EF2D85B6AC16
SHA1:	23DCC6D4B5BFE00357FD0248BB5955B8E36BB8F1
SHA-256:	99C2917EE5B2A01459A923BDD1C676F15EE73B62B87F696E6735312D26F51E12
SHA-512:	D052ECEC2839340876EB57247CFC2E777DD7F2E868DC37CD3F3F740C8DEB94917A0C9F2A4FC8229987A0B91B04726DE2D1E9F6BCBE3F9BEF0E4B7E0D7F65E12
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....L.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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
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 = 'cartItemCount=';.. 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 parentOrigin = '';.. try {.. parentHost = parent.location.hostname || '';.. parentOriginProtocol = parent.location.protocol;.. parentOrigin = parent.location.origin;.. } catch {..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\d7-de3320[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):	398770
Entropy (8bit):	5.302422750334713
Encrypted:	false
SSDEEP:	6144:d7fwtwmyU4srxCqFOp03Mw1+/cg3poEjOJ2MVuG9hRlkL:Vawmxxn917FK
MD5:	8DA101F995FA713FD329B6E42D333E05
SHA1:	831ED8D99101CA1964BEFA711689B60465951B36
SHA-256:	EF49DF74171D8E5C80F28894D824C918609AD5549CA60AB3E6023AE09C1308FD
SHA-512:	DA971DE0EC057C111CA433C3D85F2796968E96584A29510E1B08B3154C5365067888869E0552BB1440DFF40AC7C75DE0E4EA6D45DBF724EED4872E0E59A2887
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/MICROSOFT-365/_scrf/js/themes=default/c8-0b0bf1/99-5b2d94/2b-545c9f/2f-d255e3/f6-c46fbb/7e-a075ed/b0-a85e56/e7-a65b79/58-f3fc85/27-cc0f80/35-b7738f/38-a37e11/8b-1546f0/66-afd0b6/f5-7e27a5/d7-de3320?ver=2.0&_cf=20210415

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\d7-de3320[1].js	
Preview:	define("notificationBanner",["jqReady!"],function(n){"use strict";function i(){var o=document.querySelector(t.id),f,i,s,e;if(o)for(f=o.querySelectorAll(t.clsMessage),u(),i=0;i<f.length;i++)if(s=f[i].getAttribute("data-sel"),e=document.querySelector(s),e){var h=f[i].getAttribute("data-pos"),c=n(f[i]).clone(),l=c[0];r(e,h,l)}}function r(i,r,u){try{switch(r){case"replace":n(i).html(u);break;case"replaceText":n(i).text(n(u).text().trim());break;case"prepend":n(i).prepend(u);break;case"append":n(i).append(u);break;case"before":i.parentNode.insertBefore(u,i);break;case"after":default:i.parentNode.insertBefore(u,i.nextSibling)}i.classList.add(t.clsPosElement.substring(1));u.removeAttribute("data-pos");u.removeAttribute("data-sel");u.classList.add(t.clsActiveMessage.substring(1))}catch(f){}}function u(){for(var i=document.querySelectorAll(t.clsActiveMessage),n=0;n<i.length;n++)i[n].remove()}function f(){i();document.addEventListener("moduleRefreshed",i)}var t={id:"#ownb-wrapper",clsMessage:".o

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\de-bbcd6e[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):	169165
Entropy (8bit):	5.043574839315944
Encrypted:	false
SSDEEP:	3072:jzCPZkTP3bDLH0tfRqQ0xtLfj4ZDSIpTt813viY8R1j35Ap7LQZLPPJH7PAbOCxh:jlZAjLkJeTC
MD5:	FC80EE0EE4C1195A0A3573C1F22E53A8
SHA1:	82AEF853A84BE4A2C3684E67ED83F577DF61557A
SHA-256:	1B61B75684F6AC70F426526277CC6730A26CA157B7632FF0EB6A2DC4D15D94C8
SHA-512:	C367661A89582A133F88D6E141BAF95AF4C3DA42ED27954B856DD52B1D2593A9ED8B1EFE4BC176F845F5BD2FCDF14CEEA172AF7F68ACB334ADA871CD99F2BAFA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-eus-prod/west-european/shell/_scrf/css/themes=default.device=uplevel_web_pc/38-37a440/e2-7b8a97/3a-5d36b6/fb-34b6bc/20-941b48/d6-0b4b01/3c-4ad8b7/de-bbcd6e?ver=2.0&_cf=20210415
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 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 */.body{margin:0}.context-uh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\de-bbcd6e[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):	266249
Entropy (8bit):	5.07121036091961
Encrypted:	false
SSDEEP:	3072:iwzddg8HPbn/hL4fbv3DlF+ERyfJY6F0AJL55gGHjkzmEeTPNbaRgJ4J0ZRV8+uU:LLkJeTJzgRFY
MD5:	EFE9DB168447BBED87874A08FFABE5CF
SHA1:	591798AA6674FEA7A205EC3C4CD3F6A395C9F31A
SHA-256:	6674BB86357339B7FA77D6EE5D416140EBB273BCE477D682968BD8EADD0D047B
SHA-512:	64C2997C2BFC1E96420897E5F411A49BAFEA4D08C2E3801A0FD53B24BD82FD5073DA9A70D012105E194721D733FBA4735AFDA25E61A32E1B379789BF5AB46E1
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/3c-4ad8b7/44-9fa6d2/94-858fa9/90-d81c5a/97-8c42a8/33-100b4f/12-f7256c/81-8f5a7f/b5-285959/a5-15ee1d/21-7d6c87/c7-542157/c3-953460/7a-1e6e62/ae-05400e/bf-60f63e/50-55fec2/c0-379397/fd-9178b9/de-bbcd6e?ver=2.0&_cf=20210415
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{background: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 span:focus,.c-uhfh.c-sgl-stck .c-uhf-menu a:focus,.c-uhfh.c-sgl-stck .c-uhf-nav-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 soli

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\e3-082b89[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):	112710
Entropy (8bit):	5.230138550788354
Encrypted:	false
SSDEEP:	1536:uzUHQTAz7pxhX2OG+59gEkpCl+IX8BJWxFu209RhY8WOyd1EwgXA9GKamAMKrdAU:uzUzpxJIS20y9d1EwgXA95KrDDCE4+
MD5:	A09813EAC71FDD409A8B12805EAAD7AE
SHA1:	CF965D1687DE69493463FB62BE7B9FD218C244B5
SHA-256:	B9E7343D1B782B314D3054BA36B90B486070F124B4E250F45D2E6E5304CE13A0
SHA-512:	05F3026549ABDC34A7AD3FBD2B2AF2692E1A86F04459DC3B983D6622BCAF88F015BDB8B7DA98C54F7F25A05742CCA34556F80D6886D3338D2911BBFC386DFCA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\e3-082b89[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/MICROSOFT-365/_scrf/js/themes=default/2f-63ce8f/2d-7a9063/dc-7e9864/4f-5115f8/7d-266f10/4a-abd94b/6d-c07ea1/9d-b58f60/f6-aa5278/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/f8-73a5f2/79-499886/7e-cda2d3/69-13871c/6a-234a32/91-97a04f/1f-100dea/33-abe4df/17-f90ef1/e3-082b89?ver=2.0&_cf=20210415
Preview:	var __extends;define("ajaxWithAnimation",["jqReady!","jsll"],function(n,t){var i=[" <\/span><\/span><\/span><\/span><\/span><\/div>"],u=function(t,r){var u=n(t),o,f,e;u.length&&(o=(r.loaderType||"").toUpperCase(),i[1]=o==="PROGRESS"||o==="PROGRESSBAR"?"regional":o==="SPINNERLARGE"?"local f-progress-large f-center":"local f-progress-small",r.margin&&r.margin.length&&(i[3]=r.margin),f=i.join(""),e=(r.loaderPosition||"").toUpperCase(),e==="TOP"||e==="BOTTOM"?(u.addClass("ajaxloader"),e==="BOTTOM"?u.append(f):u.prepend(f)):(u.parent().addClass("ajaxloader"),e==="BEFORE"?u.before(f):u.after(f)))},f=function(t,i){var r=n(t),u;r.length&&(u=(i.loaderPosition||"").toUpperCase(),u!=="TOP"&&u!=="BOTTOM"&&(r=r.parent()),r.removeClass("ajaxloader").children().remove(".c-progress"))},r=function(i){i.refreshElement&&u(i.refreshElement,i);var r=n.extend(i,{s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\e3-082b89[2].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):	116670
Entropy (8bit):	5.226832039694129
Encrypted:	false
SSDEEP:	1536:RL0mRvoBVfpuzUHQcyAz7pxhX2OG+59gEkpCl+IX8BJWxFu209RhY8WOyd1EwgXn:fzUZpxJIS20y9d1EwgXA95KrDDCE4+
MD5:	F2670B52E7B3ED0DADC3F6FC3A67383E
SHA1:	7F282159A15C5E1F345DA8B7A3D372E174B07B36
SHA-256:	D95E30810DF759FD4A86AD6F4D3177C03035D8CE0EA476875D8970772C39252E
SHA-512:	6083D39D5DD2E15502D48787C630E0FDD8A3D98C3E87F51EE35D66EA2796FA05D0884985B7201BEEFC9D0CA3A4D07AD6A894751F185DAE5D0715120760FC1C4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/MICROSOFT-365/_scrf/js/themes=default/c9-7b8600/2f-63ce8f/45-f9a0d4/aa-dc1460/2d-7a9063/dc-7e9864/4f-5115f8/7d-266f10/4a-abd94b/6d-c07ea1/9d-b58f60/f6-aa5278/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/f8-73a5f2/79-499886/7e-cda2d3/69-13871c/6a-234a32/91-97a04f/1f-100dea/33-abe4df/17-f90ef1/e3-082b89?ver=2.0&_cf=20210415
Preview:	var __extends;require(["htmlExtensions","componentFactory","actionToggle"],function(n,t,i){var f=n.selectElements(".cui-drawer-toggle > button").concat(n.selectElements("button.cui-drawer-toggle")),e=n.selectElements(".c-drawer > button").concat(n.selectElements("button.c-drawer")),r=function(n,t){for(var o,r,e,u,i=0,f=n;i<f.length;i++)o=f[i],o.setAttribute("aria-expanded",!1);for(r=0,e=t;r<e.length;r++)u=e[r],u.setAttribute("aria-hidden",!0),u.setAttribute("style","height:0px;overflow:hidden;"),u.setAttribute("hidden","")},u=function(n,t){for(var o,r,e,u,i=0,f=n;i<f.length;i++)o=f[i],o.setAttribute("aria-expanded",!0);for(r=0,e=t;r<e.length;r++)u=e[r],u.setAttribute("aria-hidden",!1),u.setAttribute("style","height:auto;overflow:visible;"),u.removeAttribute("hidden")};t.ComponentFactory&&t.ComponentFactory.create&&(t.ComponentFactory.create([{component:i.ActionToggle,elements:f,callback:function(t){var e,i,f,o;if(t&&t.length>0)for(e=function(t){t.subscribe({onActionToggled:function(i){

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\edge[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:	downloaded
Size (bytes):	198177
Entropy (8bit):	5.131596843780732
Encrypted:	false
SSDEEP:	1536:knJQWPpE8DLHALt1QYQRpHX09blQoWifmK6HPVVi3abyqIMRsshAqhZqDZLcPyyK:GQWPpE8DLHALt1QxeqqHyqfM9juZgc9F
MD5:	9F2950B77410A5A61666785F541B42A2
SHA1:	24CFA33274284CEAC8380CA457424EC2AE19E9FC
SHA-256:	D4824255E8BD4CF18029E4D3C5D8A75E9E0EAF9F67428790E84DC4F592E7DCAA
SHA-512:	1C8CAA7DA472C7DDE45671E799B520CA2CE1C62B4CC7EBEBB7BF86C6811B3DDB8FE95BE4AF4C3800C3C17B3B24AE77EF86E4F63B2A555E33DFE141A4A89A378B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/en-us/edge?form=MI13FQ&OCID=MI13FQ
Preview:	....<!DOCTYPE html>..<html lang="en-us" class="no-js" dir="ltr" xmlns="http://www.w3.org/1999/xhtml" xmlns:og="http://ogp.me/ns#" xmlns:fb="http://www.facebook.com/2008/fbml">..<head>.. <meta charset="utf-8" />.. <meta http-equiv="X-UA-Compatible" content="IE=edge" />.. <meta http-equiv="content-language" content="en-US" />.. <title>Download Microsoft Edge Browser	Microsoft</title>.. <meta name="Title" content="Download Microsoft Edge Browser	Microsoft" />.. <meta name="Description" content="See what's new on the latest version of the Microsoft Edge browser. Explore features, rewards, and more before you download the browser today." />.. <meta name="keywords" content="internet browser, web browser, microsoft edge, download microsoft edge, microsoft edge browser" />.. <meta name="twitter:site" content="@microsoftedge" />.. <meta name="twitter:card" content="summary_large_image" />.. <meta property="og:description" content="See what's new on the

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 05:23:37.684971094 CEST	192.168.2.3	8.8.8.8	0xad81	Standard query (0)	1drv.ms	A (IP address)	IN (0x0001)
Jun 11, 2021 05:23:37.982575893 CEST	192.168.2.3	8.8.8.8	0xad29	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Jun 11, 2021 05:23:42.030456066 CEST	192.168.2.3	8.8.8.8	0xfc39	Standard query (0)	spoprod-a.akamaihd.net	A (IP address)	IN (0x0001)
Jun 11, 2021 05:23:42.036758900 CEST	192.168.2.3	8.8.8.8	0x6e05	Standard query (0)	p.sfx.ms	A (IP address)	IN (0x0001)
Jun 11, 2021 05:23:44.873541117 CEST	192.168.2.3	8.8.8.8	0x7ae0	Standard query (0)	onenoteonlinesync.onenote.com	A (IP address)	IN (0x0001)
Jun 11, 2021 05:23:48.495426893 CEST	192.168.2.3	8.8.8.8	0xf487	Standard query (0)	skyapi.onedrive.live.com	A (IP address)	IN (0x0001)
Jun 11, 2021 05:23:48.551069021 CEST	192.168.2.3	8.8.8.8	0x78c2	Standard query (0)	messaging.office.com	A (IP address)	IN (0x0001)
Jun 11, 2021 05:23:49.653269053 CEST	192.168.2.3	8.8.8.8	0x563a	Standard query (0)	c.live.com	A (IP address)	IN (0x0001)
Jun 11, 2021 05:23:54.299599886 CEST	192.168.2.3	8.8.8.8	0xe897	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Jun 11, 2021 05:23:55.189923048 CEST	192.168.2.3	8.8.8.8	0xf97c	Standard query (0)	amcdn.msftauth.net	A (IP address)	IN (0x0001)
Jun 11, 2021 05:23:55.875483036 CEST	192.168.2.3	8.8.8.8	0xc744	Standard query (0)	storage.live.com	A (IP address)	IN (0x0001)
Jun 11, 2021 05:23:56.609507084 CEST	192.168.2.3	8.8.8.8	0xad2a	Standard query (0)	www.onenote.com	A (IP address)	IN (0x0001)
Jun 11, 2021 05:24:13.690567017 CEST	192.168.2.3	8.8.8.8	0xd134	Standard query (0)	assets.adobedtm.com	A (IP address)	IN (0x0001)
Jun 11, 2021 05:24:13.729965925 CEST	192.168.2.3	8.8.8.8	0x5149	Standard query (0)	polyfill.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:24:13.741859913 CEST	192.168.2.3	8.8.8.8	0x32f1	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Jun 11, 2021 05:24:14.576503992 CEST	192.168.2.3	8.8.8.8	0xd399	Standard query (0)	js.monitor.azure.com	A (IP address)	IN (0x0001)
Jun 11, 2021 05:24:16.037184954 CEST	192.168.2.3	8.8.8.8	0x2cb6	Standard query (0)	stedgecommercialdev.blob.core.windows.net	A (IP address)	IN (0x0001)
Jun 11, 2021 05:24:16.954014063 CEST	192.168.2.3	8.8.8.8	0x3169	Standard query (0)	dc.services.visualstudio.com	A (IP address)	IN (0x0001)
Jun 11, 2021 05:24:29.534528971 CEST	192.168.2.3	8.8.8.8	0xa109	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Jun 11, 2021 05:24:29.600418091 CEST	192.168.2.3	8.8.8.8	0xe139	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)
Jun 11, 2021 05:24:38.602669954 CEST	192.168.2.3	8.8.8.8	0x3f81	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)
Jun 11, 2021 05:24:44.197338104 CEST	192.168.2.3	8.8.8.8	0x92c0	Standard query (0)	logincdn.msauth.net	A (IP address)	IN (0x0001)
Jun 11, 2021 05:24:44.584712982 CEST	192.168.2.3	8.8.8.8	0x5424	Standard query (0)	aka.ms	A (IP address)	IN (0x0001)
Jun 11, 2021 05:24:56.702722073 CEST	192.168.2.3	8.8.8.8	0x337c	Standard query (0)	amp.azure.net	A (IP address)	IN (0x0001)
Jun 11, 2021 05:24:58.930313110 CEST	192.168.2.3	8.8.8.8	0xcdfb	Standard query (0)	assets.adobedtm.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 05:25:01.481594086 CEST	192.168.2.3	8.8.8.8	0x4be5	Standard query (0)	offertoold ataprod.blob.core.windows.net	A (IP address)	IN (0x0001)
Jun 11, 2021 05:25:02.183599949 CEST	192.168.2.3	8.8.8.8	0x217c	Standard query (0)	js.monitor.azure.com	A (IP address)	IN (0x0001)
Jun 11, 2021 05:25:08.307580948 CEST	192.168.2.3	8.8.8.8	0x2622	Standard query (0)	consentreceiverfd-prod.azurefd.net	A (IP address)	IN (0x0001)
Jun 11, 2021 05:25:08.598453999 CEST	192.168.2.3	8.8.8.8	0x717	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Jun 11, 2021 05:25:16.788163900 CEST	192.168.2.3	8.8.8.8	0xd129	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)
Jun 11, 2021 05:25:16.794779062 CEST	192.168.2.3	8.8.8.8	0x4859	Standard query (0)	microsoftwindows.112.2o7.net	A (IP address)	IN (0x0001)
Jun 11, 2021 05:25:16.797184944 CEST	192.168.2.3	8.8.8.8	0x34c7	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)
Jun 11, 2021 05:25:30.903155088 CEST	192.168.2.3	8.8.8.8	0xc4ef	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)
Jun 11, 2021 05:25:30.928123951 CEST	192.168.2.3	8.8.8.8	0xa3d3	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)
Jun 11, 2021 05:25:30.980144978 CEST	192.168.2.3	8.8.8.8	0xf4b7	Standard query (0)	statics-wcus.onestore.ms	A (IP address)	IN (0x0001)
Jun 11, 2021 05:25:30.984641075 CEST	192.168.2.3	8.8.8.8	0xfc74	Standard query (0)	statics-eus.onestore.ms	A (IP address)	IN (0x0001)
Jun 11, 2021 05:25:30.988461971 CEST	192.168.2.3	8.8.8.8	0x7fef	Standard query (0)	statics-eas.onestore.ms	A (IP address)	IN (0x0001)
Jun 11, 2021 05:25:30.991552114 CEST	192.168.2.3	8.8.8.8	0xc2a5	Standard query (0)	statics-neu.onestore.ms	A (IP address)	IN (0x0001)
Jun 11, 2021 05:25:31.024806976 CEST	192.168.2.3	8.8.8.8	0x44ab	Standard query (0)	cart.production.store-web.dynamics.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 05:23:37.743525982 CEST	8.8.8.8	192.168.2.3	0xad81	No error (0)	1drv.ms		13.107.42.12	A (IP address)	IN (0x0001)
Jun 11, 2021 05:23:38.043273926 CEST	8.8.8.8	192.168.2.3	0xad29	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:23:42.092722893 CEST	8.8.8.8	192.168.2.3	0xfc39	No error (0)	spoprod-a.akamaihd.net	spoprod-a.akamaihd.net.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:23:42.111578941 CEST	8.8.8.8	192.168.2.3	0x6e05	No error (0)	p.sfx.ms	odwebp.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:23:44.984000921 CEST	8.8.8.8	192.168.2.3	0x7ae0	No error (0)	onenoteonlinesync.onenote.com	onenoteonlinesync.onenote.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:23:48.566142082 CEST	8.8.8.8	192.168.2.3	0xf487	No error (0)	skyapi.onedrive.live.com	common-geo.ha.1drv.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:23:48.566142082 CEST	8.8.8.8	192.168.2.3	0xf487	No error (0)	common-geo.ha.1drv.com	common-geo.onedrive.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:23:48.566142082 CEST	8.8.8.8	192.168.2.3	0xf487	No error (0)	am3pcor006-com.be.1drv.com	i-am3p-cor006.api.p001.1drv.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:23:48.566142082 CEST	8.8.8.8	192.168.2.3	0xf487	No error (0)	i-am3p-cor006.api.p001.1drv.com		13.104.158.180	A (IP address)	IN (0x0001)
Jun 11, 2021 05:23:48.632886887 CEST	8.8.8.8	192.168.2.3	0x78c2	No error (0)	messaging.office.com	omexmessaging.osi.office.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:23:49.727849960 CEST	8.8.8.8	192.168.2.3	0x563a	No error (0)	c.live.com	c.msn.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:23:49.727849960 CEST	8.8.8.8	192.168.2.3	0x563a	No error (0)	c.msn.com	c-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:23:54.358607054 CEST	8.8.8.8	192.168.2.3	0xe897	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 05:23:55.262795925 CEST	8.8.8.8	192.168.2.3	0xf97c	No error (0)	amcdn.msftauth.net	amcdnmsftuswe.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:23:55.942348003 CEST	8.8.8.8	192.168.2.3	0xc744	No error (0)	storage.live.com	common-geo.ha.1drv.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:23:55.942348003 CEST	8.8.8.8	192.168.2.3	0xc744	No error (0)	common-geo.ha.1drv.com	common-geo.onedrive.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:23:55.942348003 CEST	8.8.8.8	192.168.2.3	0xc744	No error (0)	am4pcor001-com.be.1drv.com	i-am4p-cor001.api.p001.1drv.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:23:55.942348003 CEST	8.8.8.8	192.168.2.3	0xc744	No error (0)	i-am4p-cor001.api.p001.1drv.com		13.105.66.144	A (IP address)	IN (0x0001)
Jun 11, 2021 05:23:56.227170944 CEST	8.8.8.8	192.168.2.3	0x8bd4	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:23:56.684303999 CEST	8.8.8.8	192.168.2.3	0xad2a	No error (0)	www.onenote.com	reverseproxy.onenote.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:24:13.755649090 CEST	8.8.8.8	192.168.2.3	0xd134	No error (0)	assets.adobedtm.com	cn-assets.adobedtm.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:24:13.787220001 CEST	8.8.8.8	192.168.2.3	0x5149	No error (0)	polyfill.io		151.101.65.26	A (IP address)	IN (0x0001)
Jun 11, 2021 05:24:13.787220001 CEST	8.8.8.8	192.168.2.3	0x5149	No error (0)	polyfill.io		151.101.129.26	A (IP address)	IN (0x0001)
Jun 11, 2021 05:24:13.787220001 CEST	8.8.8.8	192.168.2.3	0x5149	No error (0)	polyfill.io		151.101.193.26	A (IP address)	IN (0x0001)
Jun 11, 2021 05:24:13.787220001 CEST	8.8.8.8	192.168.2.3	0x5149	No error (0)	polyfill.io		151.101.1.26	A (IP address)	IN (0x0001)
Jun 11, 2021 05:24:13.805633068 CEST	8.8.8.8	192.168.2.3	0x32f1	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:24:13.876724005 CEST	8.8.8.8	192.168.2.3	0x888d	No error (0)	consentdeliveryfd.azurefd.net	firstparty-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:24:14.653637886 CEST	8.8.8.8	192.168.2.3	0xd399	No error (0)	js.monitor.azure.com	aijscdn2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:24:14.840214014 CEST	8.8.8.8	192.168.2.3	0xfe9f	No error (0)	sni1gl.wpc.gammacdn.net		152.199.21.175	A (IP address)	IN (0x0001)
Jun 11, 2021 05:24:16.128087044 CEST	8.8.8.8	192.168.2.3	0x2cb6	No error (0)	stedgecommercialdev.blob.core.windows.net	blob.dsm07prdstr05a.store.core.windows.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:24:16.128087044 CEST	8.8.8.8	192.168.2.3	0x2cb6	No error (0)	blob.dsm07prdstr05a.store.core.windows.net		20.150.89.132	A (IP address)	IN (0x0001)
Jun 11, 2021 05:24:17.030297041 CEST	8.8.8.8	192.168.2.3	0x3169	No error (0)	dc.services.visualstudio.com	dc.applicationinsights.microsoft.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:24:17.030297041 CEST	8.8.8.8	192.168.2.3	0x3169	No error (0)	dc.applicationinsights.azure.com	global.in.ai.monitor.azure.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:24:17.030297041 CEST	8.8.8.8	192.168.2.3	0x3169	No error (0)	global.in.ai.monitor.azure.com	global.in.ai.privatelink.monitor.azure.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:24:17.030297041 CEST	8.8.8.8	192.168.2.3	0x3169	No error (0)	global.in.ai.privatelink.monitor.azure.com	dc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:24:29.595304966 CEST	8.8.8.8	192.168.2.3	0xa109	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:24:29.679982901 CEST	8.8.8.8	192.168.2.3	0xe139	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:24:36.858977079 CEST	8.8.8.8	192.168.2.3	0x7506	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 05:24:38.685774088 CEST	8.8.8.8	192.168.2.3	0x3f81	No error (0)	mem.gfx.ms	cdn.account.microsoft.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:24:44.275057077 CEST	8.8.8.8	192.168.2.3	0x92c0	No error (0)	logincdn.msauth.net	lgincdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:24:44.275057077 CEST	8.8.8.8	192.168.2.3	0x92c0	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)
Jun 11, 2021 05:24:44.646800995 CEST	8.8.8.8	192.168.2.3	0x5424	No error (0)	aka.ms		95.101.18.109	A (IP address)	IN (0x0001)
Jun 11, 2021 05:24:56.765230894 CEST	8.8.8.8	192.168.2.3	0x337c	No error (0)	amp.azure.net	160c1.wpc.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:24:58.991385937 CEST	8.8.8.8	192.168.2.3	0xcdfb	No error (0)	assets.adobedtm.com	cn-assets.adobedtm.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:25:01.563988924 CEST	8.8.8.8	192.168.2.3	0x4be5	No error (0)	offertoolddataprod.blob.core.windows.net	blob.bl6prdstr14a.store.core.windows.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:25:01.563988924 CEST	8.8.8.8	192.168.2.3	0x4be5	No error (0)	blob.bl6prdstr14a.store.core.windows.net		52.239.152.74	A (IP address)	IN (0x0001)
Jun 11, 2021 05:25:02.257014036 CEST	8.8.8.8	192.168.2.3	0x217c	No error (0)	js.monitor.azure.com	aijscdn2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:25:08.381119967 CEST	8.8.8.8	192.168.2.3	0x2622	No error (0)	consentreceiverfd-prod.azurefd.net	firstparty-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:25:08.661746025 CEST	8.8.8.8	192.168.2.3	0x717	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:25:08.661746025 CEST	8.8.8.8	192.168.2.3	0x717	No error (0)	scontent.xx.fbcdn.net		31.13.92.14	A (IP address)	IN (0x0001)
Jun 11, 2021 05:25:16.854060888 CEST	8.8.8.8	192.168.2.3	0xd129	No error (0)	mem.gfx.ms	cdn.account.microsoft.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:25:16.855660915 CEST	8.8.8.8	192.168.2.3	0x4859	No error (0)	microsoftwindows.112.2o7.net		13.36.218.177	A (IP address)	IN (0x0001)
Jun 11, 2021 05:25:16.855660915 CEST	8.8.8.8	192.168.2.3	0x4859	No error (0)	microsoftwindows.112.2o7.net		15.236.176.210	A (IP address)	IN (0x0001)
Jun 11, 2021 05:25:16.855660915 CEST	8.8.8.8	192.168.2.3	0x4859	No error (0)	microsoftwindows.112.2o7.net		15.188.95.229	A (IP address)	IN (0x0001)
Jun 11, 2021 05:25:16.859652996 CEST	8.8.8.8	192.168.2.3	0x34c7	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:25:30.962280989 CEST	8.8.8.8	192.168.2.3	0xc4ef	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:25:30.987489939 CEST	8.8.8.8	192.168.2.3	0xa3d3	No error (0)	mem.gfx.ms	cdn.account.microsoft.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:25:31.040647984 CEST	8.8.8.8	192.168.2.3	0xf4b7	No error (0)	statics-wcus.onestore.ms	statics.onestore.ms.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:25:31.047518969 CEST	8.8.8.8	192.168.2.3	0xfc74	No error (0)	statics-eus.onestore.ms	statics.onestore.ms.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:25:31.049056053 CEST	8.8.8.8	192.168.2.3	0x7fef	No error (0)	statics-eas.onestore.ms	statics.onestore.ms.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:25:31.054910898 CEST	8.8.8.8	192.168.2.3	0xc2a5	No error (0)	statics-neu.onestore.ms	statics.onestore.ms.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:25:31.103442907 CEST	8.8.8.8	192.168.2.3	0x44ab	No error (0)	cart.production.store-web.dynamics.com	storeweb-cart-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 05:25:31.103442907 CEST	8.8.8.8	192.168.2.3	0x44ab	No error (0)	cart.northeurope.production.store-web.dynamics.com	sw-prod-appgwpublicip-northeurope.northeurope.cloudapp.azure.com		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
Jun 11, 2021 05:24:14.057090998 CEST	151.101.65.26	443	192.168.2.3	49791	CN=polyfill.io CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri Jun 04 21:31:46 CEST 2021	Wed Jul 06 21:31:45 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
							Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jun 11, 2021 05:24:14.235508919 CEST	151.101.65.26	443	192.168.2.3	49790	CN=polyfill.io CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri Jun 04 21:31:46 CEST 2021	Wed Jul 06 21:31:45 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
							Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jun 11, 2021 05:24:14.975788116 CEST	152.199.21.175	443	192.168.2.3	49815	CN=sni1e6ffgl.wpc.edgecastcdn.net, OU=SecOps, O="Verizon Digital Media Services, Inc.", L=Los Angeles, 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	Thu Apr 16 02:00:00 CEST 2020	Thu Apr 21 14:00:00 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
							Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					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		
Jun 11, 2021 05:24:14.975938082 CEST	152.199.21.175	443	192.168.2.3	49814	CN=sni1e6ffgl.wpc.edgecastcdn.net, OU=SecOps, O="Verizon Digital Media Services, Inc.", L=Los Angeles, 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	Thu Apr 16 02:00:00 CEST 2020	Thu Apr 21 14:00:00 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
							Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 11, 2021 05:24:44.371618032 CEST	192.229.221.185	443	192.168.2.3	49869	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	Thu May 13 02:00:00 CEST 2021 Wed Sep 23 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Sat May 14 01:59:59 CEST 2022 Mon Sep 23 01:59:59 CEST 2030 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	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
					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		
Jun 11, 2021 05:24:44.371870995 CEST	192.229.221.185	443	192.168.2.3	49870	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	Thu May 13 02:00:00 CEST 2021 Wed Sep 23 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Sat May 14 01:59:59 CEST 2022 Mon Sep 23 01:59:59 CEST 2030 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	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
					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		
Jun 11, 2021 05:24:44.773072958 CEST	95.101.18.109	443	192.168.2.3	49872	CN=go.microsoft.com, OU=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft RSA TLS CA 01, O=Microsoft Corporation, C=US	CN=Microsoft RSA TLS CA 01, O=Microsoft Corporation, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jan 07 22:45:54 CET 2021 Wed Jul 22 01:00:00 CEST 2020	Fri Jan 07 22:45:54 CET 2022 Tue Oct 08 09:00:00 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 RSA TLS CA 01, O=Microsoft Corporation, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Jul 22 01:00:00 CEST 2020	Tue Oct 08 09:00:00 CEST 2024		
Jun 11, 2021 05:24:44.773669958 CEST	95.101.18.109	443	192.168.2.3	49871	CN=go.microsoft.com, OU=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft RSA TLS CA 01, O=Microsoft Corporation, C=US	CN=Microsoft RSA TLS CA 01, O=Microsoft Corporation, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jan 07 22:45:54 CET 2021 Wed Jul 22 01:00:00 CEST 2020	Fri Jan 07 22:45:54 CET 2022 Tue Oct 08 09:00:00 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 RSA TLS CA 01, O=Microsoft Corporation, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Jul 22 01:00:00 CEST 2020	Tue Oct 08 09:00:00 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
Jun 11, 2021 05:25:08.758083105 CEST	31.13.92.14	443	192.168.2.3	49901	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	Wed May 26 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 25 01:59:59 CEST 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		
Jun 11, 2021 05:25:08.765038967 CEST	31.13.92.14	443	192.168.2.3	49900	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	Wed May 26 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 25 01:59:59 CEST 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		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5424 Parent PID: 792

General

Start time:	05:23:35
Start date:	11/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7a1390000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 5124 Parent PID: 5424

General

Start time:	05:23:36
Start date:	11/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5424 CREDAT:17410 /prefetch:2
Imagebase:	0xad0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: dllhost.exe PID: 3468 Parent PID: 792

General

Start time:	05:24:00
Start date:	11/06/2021
Path:	C:\Windows\System32\dllhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\DllHost.exe /Processid:{49F171DD-B51A-40D3-9A6C-52D674CC729D}
Imagebase:	0x7ff7bc440000
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

Show Windows behavior

Analysis Process: explorer.exe PID: 3388 Parent PID: 3468

General

Start time:	05:24:01
Start date:	11/06/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
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 Show Windows behavior

Analysis Process: iexplore.exe PID: 488 Parent PID: 5424

General

Start time:	05:24:11
Start date:	11/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5424 CREDAT:82960 /prefetch:2
Imagebase:	0xad0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 1392 Parent PID: 5424

General

Start time:	05:24:27
Start date:	11/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5424 CREDAT:17438 /prefetch:2
Imagebase:	0xad0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Disassembly

Code Analysis