

JOeSandbox Cloud BASIC



ID: 339263

Cookbook: browseurl.jbs

Time: 19:06:51

Date: 13/01/2021

Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents	2
Analysis Report https://cmrinsure-my.sharepoint.com/:b:/g/personal/seccles_cmrinsurance_com/EXDgzrrmhc1GnNui_DLzzBkBEUB0mDIJ3B08lrE-XQmbmg?e=4%3avE67Ot&at=9	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Startup	3
Malware Configuration	3
Yara Overview	3
Dropped Files	3
Sigma Overview	3
Signature Overview	4
Phishing:	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	7
Domains and IPs	8
Contacted Domains	8
URLs from Memory and Binaries	8
Contacted IPs	13
Public	14
Private	14
General Information	14
Simulations	17
Behavior and APIs	17
Joe Sandbox View / Context	17
IPs	17
Domains	17
ASN	17
JA3 Fingerprints	17
Dropped Files	17
Created / dropped Files	17
Static File Info	50
No static file info	50
Network Behavior	50
Network Port Distribution	50
TCP Packets	51
UDP Packets	52
DNS Queries	55
DNS Answers	56
HTTPS Packets	57
Code Manipulations	58
Statistics	58
Behavior	58
System Behavior	59
Analysis Process: iexplore.exe PID: 5364 Parent PID: 792	59
General	59
File Activities	59
Registry Activities	59
Analysis Process: iexplore.exe PID: 1064 Parent PID: 5364	59
General	60
File Activities	60
Registry Activities	60
Analysis Process: dllhost.exe PID: 2168 Parent PID: 792	60
General	60
File Activities	60
Analysis Process: explorer.exe PID: 3388 Parent PID: 2168	60
General	60
Analysis Process: iexplore.exe PID: 2788 Parent PID: 5364	61
General	61
File Activities	61
Registry Activities	61
Disassembly	61
Code Analysis	61

Analysis Report https://cmrinsure-my.sharepoint.com/:b...

Overview

General Information

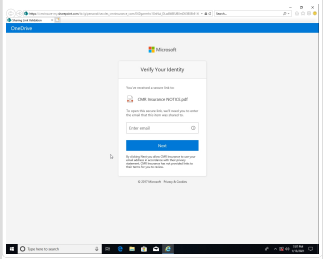
Sample URL:

https://cmrinsure-my.sharepoint.com/:b/g/personal/seccles_cmrrinsurance_com...urance_com/EXDgzrmhc1GnNui_DLzzBkBEUB0mDIJ3B08lrE-XQmbmg?e=4%3avE67Ot&at=9

Analysis ID:

339263

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

HTMLPhisher

Score:

56

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Yara detected HtmlPhish_10

Phishing site detected (based on im...

Phishing site detected (based on log...

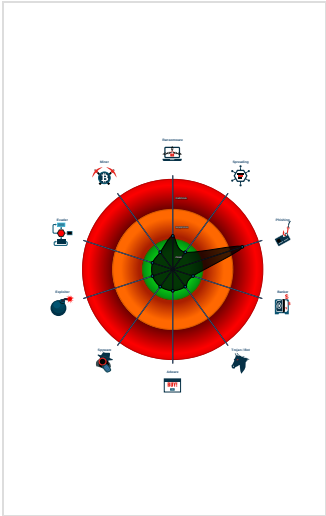
HTML body contains low number of ...

HTML title does not match URL

Monitors certain registry keys / valu...

Submit button contains javascript call

Classification



Startup

System is w10x64

iexplore.exe (PID: 5364 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)

iexplore.exe (PID: 1064 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5364 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)

iexplore.exe (PID: 2788 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5364 CREDAT:17418 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)

dllhost.exe (PID: 2168 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

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\EXDgzrmhc1GnNui_DLzzBkBEUB0mDIJ3B08lrE-XQmbmg[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

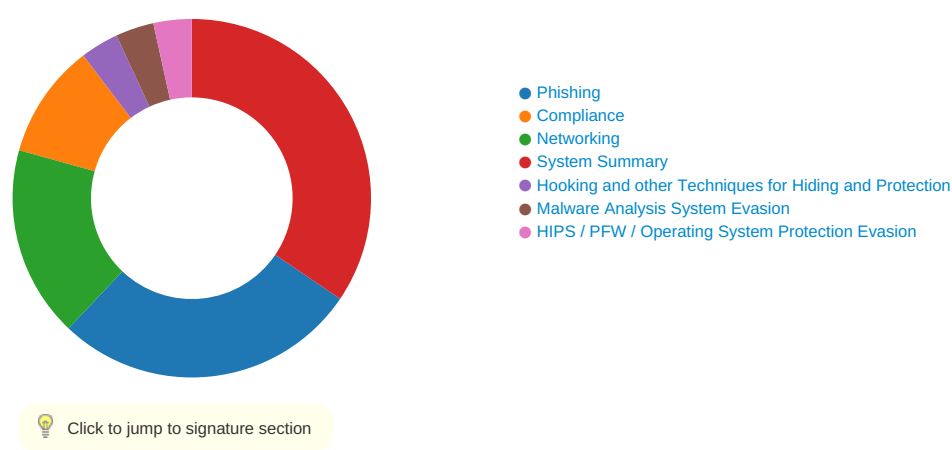
Sigma Overview

No Sigma rule has matched

Copyright null 2021

Page 3 of 61

Signature Overview



Phishing:

Yara detected HtmlPhish_10

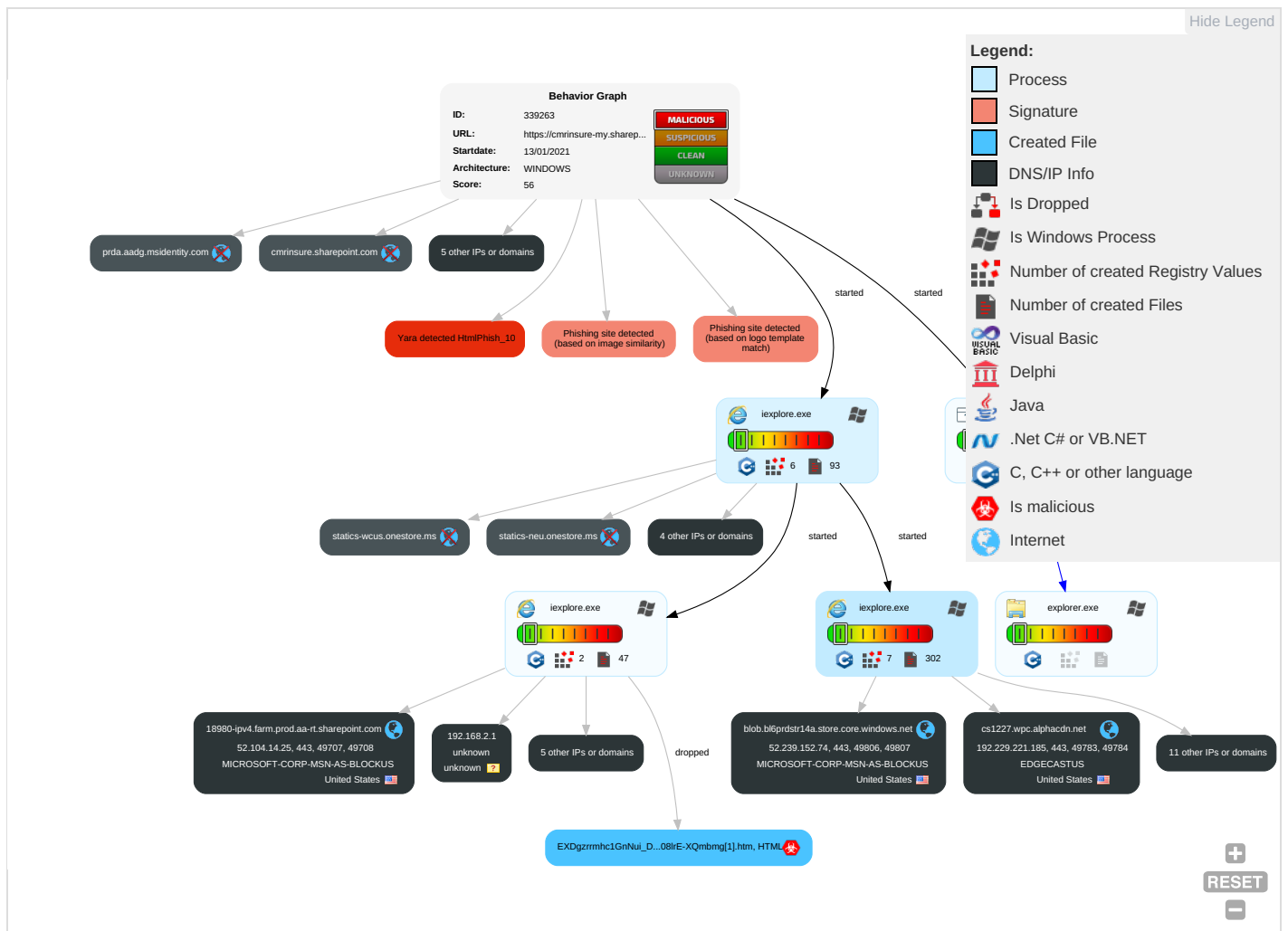
Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Scripting 1	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partitic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockot
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

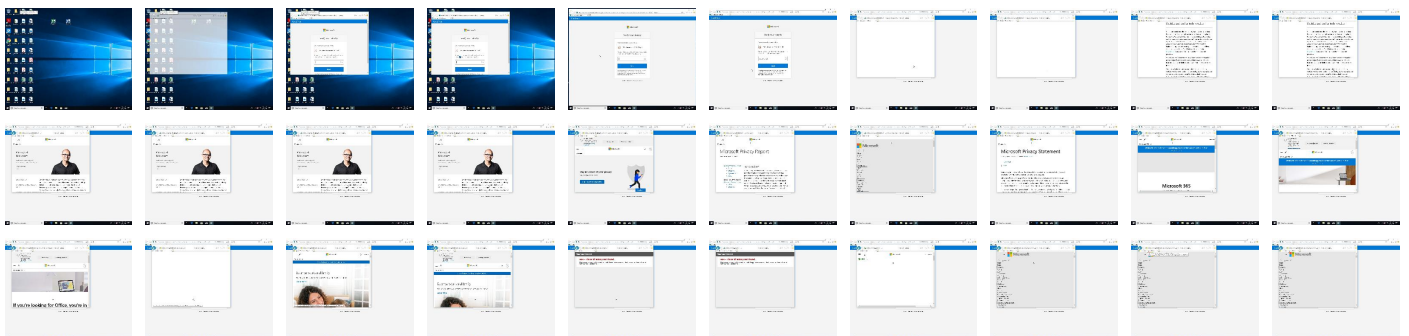
Behavior Graph

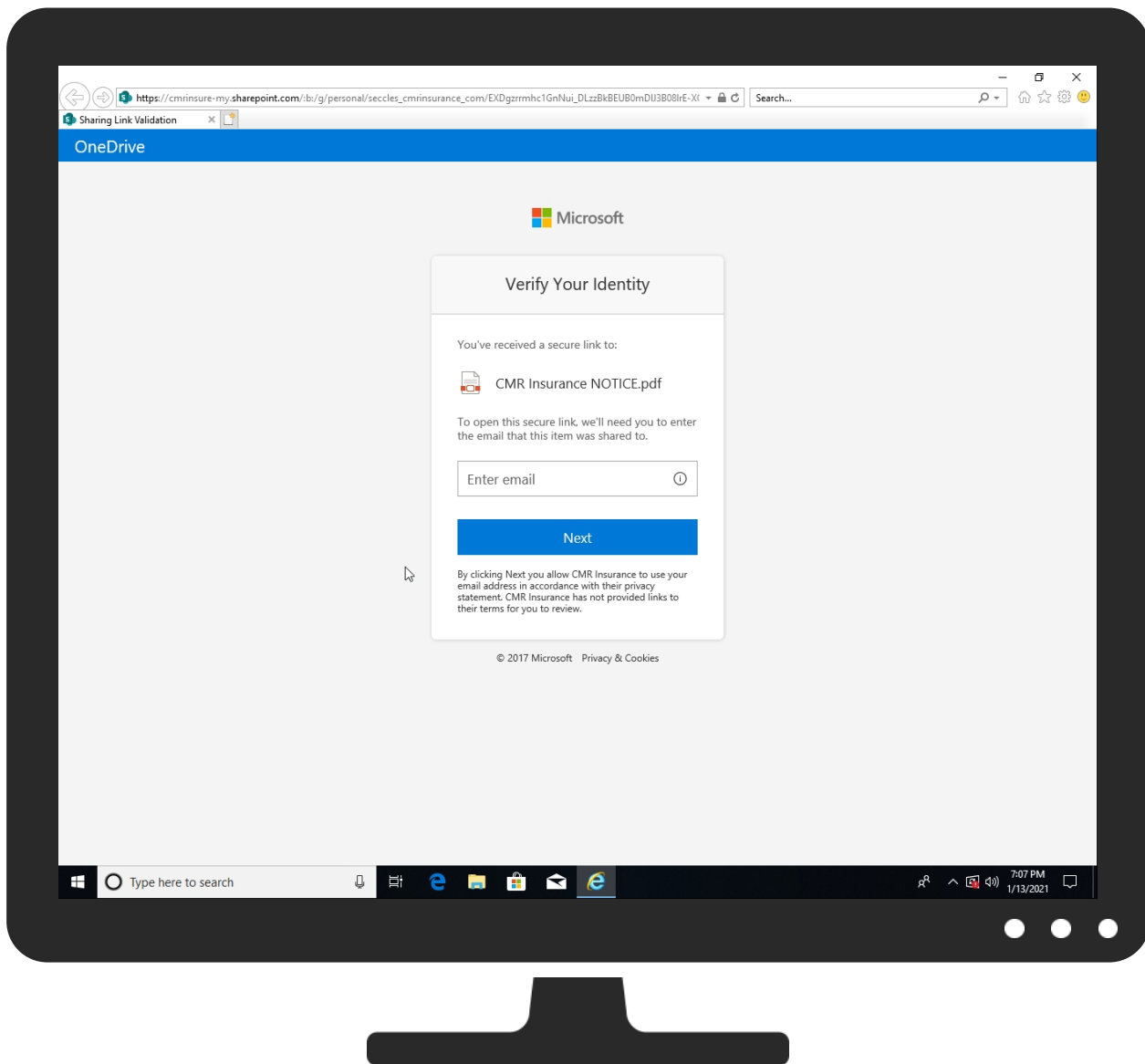


Screenshots

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
https://cmrinsure-my.sharepoint.com/:b:/g/personal/seccles_cminsurance_com/EXDgzrmhc1GnNui_DLzzBkBEUB0mDIJ3B08lrE-XQmbmg?e=4%3avE67Ot&at=9	0%	Virustotal		Browse
https://cmrinsure-my.sharepoint.com/:b:/g/personal/seccles_cminsurance_com/EXDgzrmhc1GnNui_DLzzBkBEUB0mDIJ3B08lrE-XQmbmg?e=4%3avE67Ot&at=9	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cs1227.wpc.alphacdn.net	0%	Virustotal		Browse
logincdn.msauth.net	0%	Virustotal		Browse
statics-eas.onestore.ms	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://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://www.youradchoices.ca/fr	0%	URL Reputation	safe	
http://https://www.youradchoices.ca/fr	0%	URL Reputation	safe	
http://https://www.youradchoices.ca/fr	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPIease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPIease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPIease	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	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	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://fontello.com/icons/RegularIconsVersion	0%	URL Reputation	safe	
http://fontello.com/icons/RegularIconsVersion	0%	URL Reputation	safe	
http://fontello.com/icons/RegularIconsVersion	0%	URL Reputation	safe	
http://https://cmrinsure-my.sharepoint.com/favicon.ico	0%	Avira URL Cloud	safe	
http://https://cmrinsure-my.sharepoint.com/_layouts/15/images/favicon.ico?rev=47	0%	Avira URL Cloud	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://www.michaelbromley.co.uk/blog/193/a-note-on-touch-pointer-events-in-ie11	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
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
aka.ms	23.211.149.25	true	false		high
18980-ipv4.farm.prod.aa-rt.sharepoint.com	52.104.14.25	true	false		unknown
logincdn.msauth.net	unknown	unknown	false	0%, Virustotal, Browse	unknown
www.xbox.com	unknown	unknown	false		high
assets.adobedtm.com	unknown	unknown	false		high
statics-eas.onestore.ms	unknown	unknown	false	0%, Virustotal, Browse	unknown
assets.onestore.ms	unknown	unknown	false		unknown
ajax.aspnetcdn.com	unknown	unknown	false		high
mem.gfx.ms	unknown	unknown	false		unknown
statics-neu.onestore.ms	unknown	unknown	false		unknown
statics-wcus.onestore.ms	unknown	unknown	false		unknown
statics-eus.onestore.ms	unknown	unknown	false		unknown
amp.azure.net	unknown	unknown	false		high
cmrinsure-my.sharepoint.com	unknown	unknown	false		unknown
spoprod-a.akamaihd.net	unknown	unknown	false		high
cdn.onenote.net	unknown	unknown	false		unknown
offertooldataprod.blob.core.windows.net	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	iexplore.exe, 00000001.00000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://www.mercadolivre.com.br/	iexplore.exe, 00000001.00000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	iexplore.exe, 00000001.00000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://compass-ssl.xbox.com/assets/61/db/61db4e12-c19f-4077-9662-7b12324b840f.jpg?n=The-Falconeer_S	allContent2[1].js.14.dr	false		high
http://https://compass-ssl.xbox.com/assets/ca/ba/caba6646-02b5-4ccd-9b16-7f230ce43166.svg?n=Homepage-FY20_H	allContent2[1].js.14.dr	false		high
http://www.dailymail.co.uk/	iexplore.exe, 00000001.00000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://gear.xbox.com/en-us/	allContent2[1].js.14.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://account.xbox.com/xbox/accountsignin?returnurl=https%3A%2F%2Fwww.xbox.com%2Far-ae	allContent2[1].js.14.dr	false		high
http://https://www.youradchoices.ca/fr	privacystatement[1].htm.14.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://codepen.io/tigt/post/optimizing-svgs-in-data-uris	mwf-main.var[1].js.14.dr	false		high
http://https://compass-ssl.xbox.com/assets/88/1e/881e4aa7-8f37-43b5-8cb1-a9204804dccb.jpg?n=006517_Page-Her	allHeroes2[1].js.14.dr	false		high
http://www.asp.net/ajaxlibrary/CDN.ashx	en-US[1].htm.14.dr, privacystatement[1].htm.14.dr	false		high
http://www.fontbureau.com/designers	explorer.exe, 00000008.00000000 0.262454414.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://https://compass-ssl.xbox.com/assets/d6/ff/d6ff1c1b-58ca-4491-b5fd-9f5e9c2ee7a9.jpg?n=COD-BOCW_Small-	allContent2[1].js.14.dr	false		high
http://https://www.xbox.com/accessories/controllers/xbox-wireless-controller	allContent2[1].js.14.dr	false		high
http://https://www.xbox.com/games/hitman-3	allContent2[1].js.14.dr	false		high
http://fr.search.yahoo.com/	ieexplore.exe, 00000001.00000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://in.search.yahoo.com/	ieexplore.exe, 00000001.00000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://github.com/jrburke/requirejs	require[1].js.2.dr	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	ieexplore.exe, 00000001.00000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://https://compass-ssl.xbox.com/assets/29/68/2968abbc-7a2e-4a3c-a81e-de73cbab8f23.jpg?n=Power-Your-Drea	allContent2[1].js.14.dr	false		high
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000008.00000000 0.262454414.0000000008B46000.0 0000002.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://account.xbox.com/xbox/accountsignin?returnurl=https%3A%2F%2Fwww.xbox.com%2Ftr-tr	allContent2[1].js.14.dr	false		high
http://msk.afisha.ru/	ieexplore.exe, 00000001.00000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	ieexplore.exe, 00000001.00000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/13167260817d/RC5548547466864ee2ab73cca512147d7	RC5548547466864ee2ab73cca512147d77-source.min[1].js.14.dr	false		high
http://https://www.xbox.com/en-US/-us/surface365/microsoft-office47	ieexplore.exe, 00000001.00000000 2.464814405.000001DBB36FF000.0 0000004.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	ieexplore.exe, 00000001.00000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://www.etmall.com.tw/favicon.ico	ieexplore.exe, 00000001.00000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown

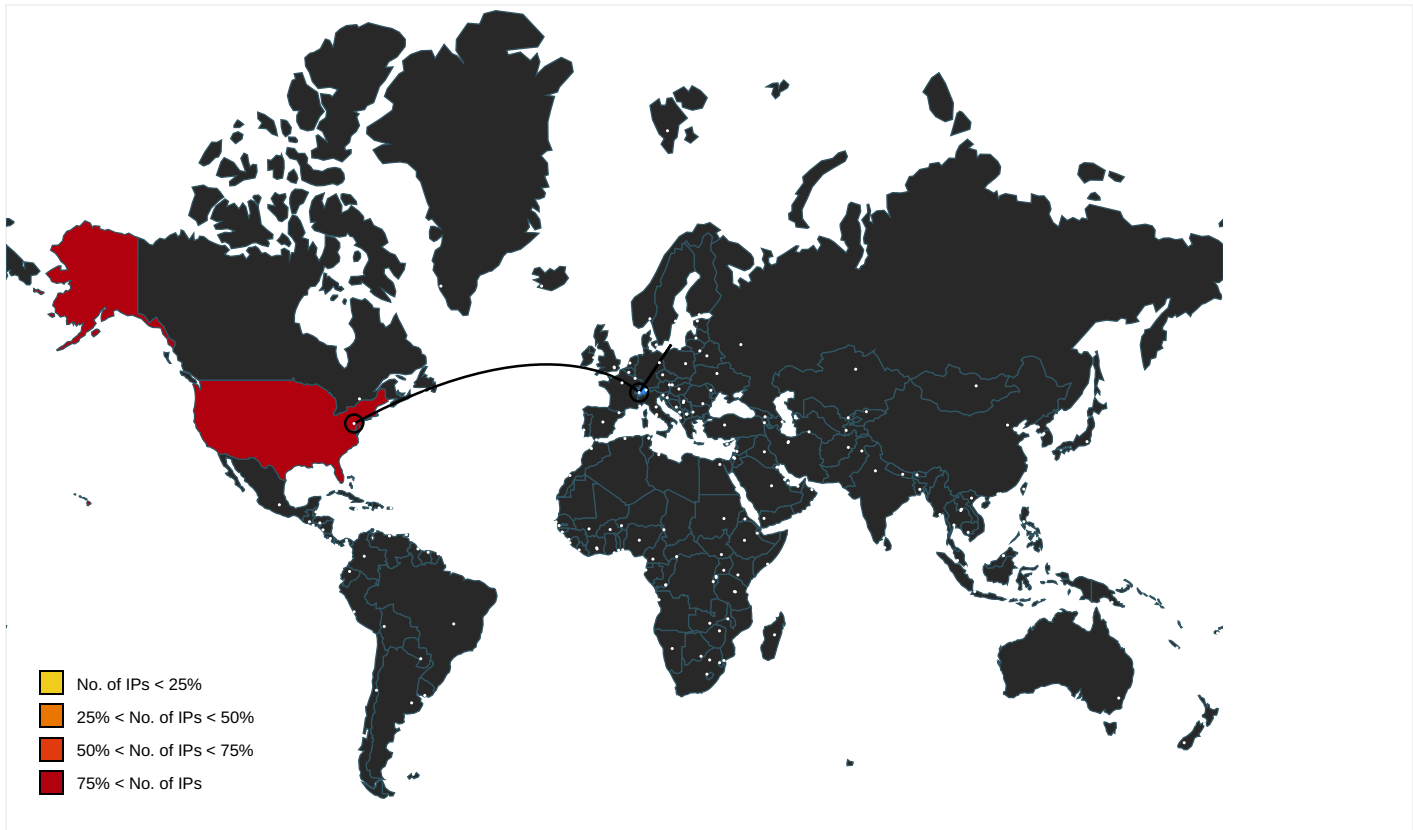
Name	Source	Malicious	Antivirus Detection	Reputation
http://it.search.dada.net/favicon.ico	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://www.xbox.com/managedatacollection	privacystatement[1].htm.14.dr	false		high
http://https://compass-ssl.xbox.com/assets/3a/41/3a4199da-4f90-4701-9804-37073bd8c2ee.mp4?n=Grounded_HP-FAT	contentPop2[1].js.14.dr	false		high
http://search.hanafos.com/favicon.ico	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false	Avira URL Cloud: safe	unknown
http://https://css-tricks.com/probably-dont-base64-svg/	mwf-main.var[1].js.14.dr	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000008.0000000 0.264046979.00000000E2B3000.0 0000002.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://buscar.ozu.es/	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false	Avira URL Cloud: safe	unknown
http://https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protectio	privacystatement[1].htm.14.dr	false		high
http://account.xbox.com/xbox/accountsignin?returnurl=https%3A%2F%2Fwww.xbox.com%2Fhe-il	allContent2[1].js.14.dr	false		high
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://www.ask.com/	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://https://www.xbox.com/en-US/	{BC5DD018-5615-11EB-90E4-ECF4B B862DED}.dat.1.dr	false		high
http://www.google.it/	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://https://compass-ssl.xbox.com/assets/1d/66/1d66cdce-df64-4204-b2de-072a60a95bdb.jpg?n=Injustice-2_Pag	allHeroes2[1].js.14.dr	false		high
http://search.auction.co.kr/	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://www.amazon.de/	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://fontello.com/iconsRegulariconsiconsVersion	icons[1].eot.14.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://sads.myspace.com/	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://account.xbox.com/xbox/accountsignin?returnurl=https%3A%2F%2Fwww.xbox.com%2Fes-mx	allContent2[1].js.14.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cmrinsure-my.sharepoint.com/favicon.ico	iexplore.exe, 00000001.0000000 2.452209619.000001DBAFDF8000.0 0000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://https://cmrinsure-my.sharepoint.com/_layouts/15/images/favicon.ico?rev=47	imagestore.dat.2.dr	false	Avira URL Cloud: safe	unknown
http://https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/13167260817d/RCD898c8a8376b41f88f24c93b8645f17	RCD898c8a8376b41f88f24c93b8645f178-source.min[1].js.14.dr	false		high
http://www.pchome.com.tw/favicon.ico	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://google.pchome.com.tw/	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://www.rambler.ru/favicon.ico	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://https://compass-ssl.xbox.com/assets/88/54/88549de9-e881-40bf-b4ec-17f176b8b4cf.mp4?n=333099_Small-To	contentPop2[1].js.14.dr	false		high
http://uk.search.yahoo.com/	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://www.ozu.es/favicon.ico	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false	Avira URL Cloud: safe	unknown
http://https://signin.kissmetrics.com/privacy/#controls	privacystatement[1].htm.14.dr	false		high
http://search.sify.com/	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://www.michaelbromley.co.uk/blog/193/a-note-on-touch-pointer-events-in-ie11	mwf-main.var[1].js.14.dr	false	Avira URL Cloud: safe	unknown
http://openimage.interpark.com/interpark.ico	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://www.gmarket.co.kr/	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://account.xbox.com/xbox/accountsignin?returnurl=https%3A%2F%2Fwww.xbox.com%2Fen-ca	allContent2[1].js.14.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000008.0000000 0.262454414.0000000008B46000.0 0000002.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://search.nifty.com/	ieexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://https://compass-ssl.xbox.com/assets/7b/30/7b30e02e-472a-46a6-b0fe-76a971dcec19.gif?n=Grounded_GLP-Ci	contentPop2[1].js.14.dr	false		high
http://www.google.si/	ieexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://www.soso.com/	ieexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://https://www.xbox.com/en-US/i	ieexplore.exe, 00000001.0000000 2.451614476.000001DBAFA80000.0 0000004.00000001.sdmp	false		high
http://https://www.xbox.com/en-US/k	ieexplore.exe, 00000001.0000000 2.452221961.000001DBAFE04000.0 0000004.00000001.sdmp	false		high
http://https://www.xbox.com/games/call-of-duty-black-ops-cold-war#whatsnew	allContent2[1].js.14.dr	false		high
http://account.xbox.com/xbox/accountsignin?returnurl=https%3A%2F%2Fwww.xbox.com%2Fpt-br	allContent2[1].js.14.dr	false		high
http://busca.orange.es/	ieexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	ieexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://www.twitter.com/	ieexplore.exe, 00000001.0000000 2.451477201.000001DBAFA0A000.0 0000004.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	ieexplore.exe, 00000001.0000000 2.448873122.000001DBAF280000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.263866124.00000 0000E1C0000.00000002.00000001. sdmp	false		high
http://www.target.com/	ieexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://https://www.xbox.com/en-US/b	ieexplore.exe, 00000001.0000000 2.451803229.000001DBAFB2D000.0 0000004.00000001.sdmp	false		high
http://https://www.xbox.com/en-US/d	ieexplore.exe, 00000001.0000000 2.451614476.000001DBAFA80000.0 0000004.00000001.sdmp	false		high
http://https://www.xbox.com/favicon.ico	ieexplore.exe, 00000001.0000000 2.451803229.000001DBAFB2D000.0 0000004.00000001.sdmp, imagest ore.dat.14.dr	false		high
http://search.orange.co.uk/favicon.ico	ieexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://www.iask.com/	ieexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://compass-ssl.xbox.com/assets/61/27/6127707e-15f9-43b1-b2f4-67069007436f.mp4?n=333099_Large-To	contentPop2[1].js.14.dr	false		high
http://https://spoprod-a.akamaihd.net/files/fabric-cdn-prod_20201008.001/assets/item-types/	spoguestaccess-a0017cc2[1].js.2.dr	false		high
http://https://www.appsflyer.com/optout	privacystatement[1].htm.14.dr	false		high
http://https://www.xbox.com/en-US/2	iexplore.exe, 00000001.0000000 2.451803229.000001DBAFB2D000.0 0000004.00000001.sdmp	false		high
http://https://www.xbox.com/en-US/cLMMEX	iexplore.exe, 00000001.0000000 2.464814405.000001DBB36FF000.0 0000004.00000001.sdmp	false		high
http://search.centrum.cz/favicon.ico	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://account.xbox.com/xbox/accountsignin?returnurl=https%3A%2F%2Fwww.xbox.com%2Fpl-pl	allContent2[1].js.14.dr	false		high
http://service2.bfast.com/	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ariadna.elmundo.es/	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://https://compass-ssl.xbox.com/assets/a2/d5/a2d59139-74fd-482a-b940-3bfc78e655a0.jpg?n=COD-BOCW_Small-	allContent2[1].js.14.dr	false		high
http://www.news.com.au/favicon.ico	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.cdiscout.com/	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high
http://www.tiscali.it/favicon.ico	iexplore.exe, 00000001.0000000 2.449842995.000001DBAF373000.0 0000002.00000001.sdmp, explorer.exe, 00000008.00000000.264046979.00000 0000E2B3000.00000002.00000001. sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.239.152.74	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.104.14.25	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
192.229.221.185	unknown	United States		15133	EDGECASTUS	false
23.211.149.25	unknown	United States		16625	AKAMAI-ASUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339263
Start date:	13.01.2021
Start time:	19:06:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://cmrinsure-my.sharepoint.com/:b:/g/personal/seccles_cmrrinsurance_com/EXDgzrrmhc1GnNui_DLzzBkBEUB0mDIJ3B08lrE-XQmbmg?e=4%3avE67Ot&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:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0

Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.phis.win@6/289@19/5
EGA Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://go.microsoft.com/fwlink/?linkid=845480 • Browsing link: https://go.microsoft.com/fwlink/p/?linkid=2126808 • Browsing link: https://go.microsoft.com/fwlink/p/?linkid=2126809 • Browsing link: https://go.microsoft.com/fwlink/p/?linkid=2126907 • Browsing link: https://go.microsoft.com/fwlink/p/?linkid=2126908 • Browsing link: https://go.microsoft.com/fwlink/p/?linkid=2126810 • Browsing link: https://www.microsoft.com/microsoft-365 • Browsing link: https://www.microsoft.com/en-us/microsoft-365/microsoft-office • Browsing link: https://www.microsoft.com/en-us/windows/ • Browsing link: https://www.microsoft.com/en-us/surface • Browsing link: https://www.xbox.com/ • Browsing link: https://www.microsoft.com/en-us/store/b/sale?icid=gm_nav_L0_salepage
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, dllhost.exe, BackgroundTransferHost.exe, ielowutil.exe, HxTsr.exe, RuntimeBroker.exe, wermgr.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.43.193.48, 88.221.62.148, 2.20.143.23, 2.20.142.202, 92.122.213.248, 92.122.213.216, 2.17.179.193, 84.53.167.113, 20.190.129.24, 40.126.1.145, 20.190.129.160, 20.190.129.17, 40.126.1.128, 20.190.129.130, 40.126.1.166, 20.190.129.133, 93.184.220.29, 204.79.197.200, 13.107.21.200, 51.104.139.180, 152.199.19.161, 23.210.248.85, 23.210.249.50, 92.122.145.53, 152.199.19.160, 92.122.213.194, 92.122.213.240, 23.210.249.93, 84.53.167.109, 92.122.213.247, 92.122.213.200, 92.122.213.219, 23.201.255.153, 20.190.129.128, 20.190.129.2, 40.126.1.142, 205.185.216.42, 205.185.216.10, 92.122.213.193, 92.122.213.176, 2.17.185.83, 13.107.246.13, 23.50.99.143, 65.55.44.109, 92.122.145.220, 92.122.213.154, 92.122.213.163, 92.122.213.195, 23.205.179.153, 23.210.248.45, 92.122.144.209, 51.11.168.160 • Excluded domains from analysis (whitelisted): assets.onestore.ms.edgekey.net, www.xbox.com.akadns.net, cn-assets.adobedtm.com.edgekey.net, i-s-microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, cdn.onenote.net.edgekey.net, www.tm.a.prd.aadg.trafficmanager.net, a1945.g2.akamai.net, star-azurefd-prod.trafficmanager.net, statics-marketingites-eus-ms-com.akamaized.net, au-bg-shim.trafficmanager.net, www.bing.com, dual-a-0001.a-msedge.net, account.microsoft.com.edgekey.net, compass-ssl.microsoft.com, lgincdnvzeuno.ec.azureedge.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, assets.onestore.ms.akadns.net, statics.onestore.ms.edgekey.net, skype-dataprdcolcus15.cloudapp.net, c-

s.cms.ms.akadns.net, lgincdn.trafficmanager.net, cdn.account.microsoft.com.akadns.net, a1531.g2.akamai.net, e1553.dspg.akamaiedge.net, spoprod-a.akamaihd.net.edgesuite.net, c.s-microsoft.com-c.edgekey.net, compass-ssl.microsoft.com.edgekey.net, cs9.wpc.v0cdn.net, a1985.g2.akamai.net, e9412.b.akamaiedge.net, compass-ssl.microsoft.com.nsatc.net, i.s-microsoft.com, e15275.g.akamaiedge.net, storeedgefd.xbetservices.akadns.net, statica.akamai.odsp.cdn.office.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, e1822.dspb.akamaiedge.net, go.microsoft.com, prod-video-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, storeedgefd.dsx.mp.microsoft.com, 160c1.wpc.azureedge.net, ie9comview.vo.msecnd.net, cs22.wpc.v0cdn.net, mem.gfx.ms.edgekey.net, tile-service.weather.microsoft.com, cds.d2s7q6s2.hwcdn.net, login.msa.msidentity.com, statics-uhf-eus.akamaized.net, c.s-microsoft.com, e7808.dscg.akamaiedge.net, go.microsoft.com.edgekey.net, a1963.g2.akamai.net, az725175.vo.msecnd.net, e13678.dspb.akamaiedge.net, query.prod.cms.rt.microsoft.com, wcpstatic.microsoft.com, mmf-service.akamaized.net, cs9.wac.phicdn.net, arc.msn.com.nsatc.net, e13678.dscb.akamaiedge.net, www.tm.lg.prod.aadmsa.akadns.net, e11290.dspg.akamaiedge.net, www.microsoft.com-c-3.edgekey.net, query.prod.cms.rt.microsoft.com.edgekey.net, ocsp.digicert.com, wildcard.weather.microsoft.com.edgekey.net, login.live.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, e11070.b.akamaiedge.net, watson.telemetry.microsoft.com, a1778.g2.akamai.net, standard.t-0003.t-msedge.net, e10583.dspg.akamaiedge.net, fs.microsoft.com, statica.akamai.odsp.cdn.office.net-c.edgesuite.net, statics-marketing-sites-wcus-ms-com.akamaized.net, www.tm.a.prd.aadg.akadns.net, web.vortex.data.trafficmanager.net, e10583.g.akamaiedge.net, wildcard.xbox.com.edgekey.net, t-0003.t-msedge.net, e55.dspb.akamaiedge.net, dub2.current.a.prd.aadg.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, privacy.microsoft.com.edgekey.net, www.tm.lg.prod.aadmsa.trafficmanager.net, e2699.dspg.akamaiedge.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, globalredir.akadns.net, account.microsoft.com, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www.microsoft.com-c-3.edgekey.net, globalredir.akadns.net, mscomajax.vo.msecnd.net, img-prod-cms-rt-microsoft-com.akamaized.net, statica.akamai.odsp.cdn.office.net-c.edgesuite.net, globalredir.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, Edge-Prod-FRr3.ctrl.t-0003.t-msedge.net, web.vortex.data.microsoft.com, lgincdnvzeuno.azureedge.net, skype-dataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, privacy.microsoft.com, a1512.dscg2.akamai.net, e16646.dscg.akamaiedge.net, e13678.dscg.akamaiedge.net, www.microsoft.com, a1813.dscd.akamai.net

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

Simulations

Behavior and APIs

Time	Type	Description
19:07:57	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\KTDAP97H\www.microsoft[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	135
Entropy (8bit):	4.728453743534065
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsnObemKmlULF0VqHIJR3KaWX69qSRD2LKb:JFK1rUFjgemKm6GVqHIJR3/Q6lDb
MD5:	3BACA892045CB07AF2C542E580917736
SHA1:	E8D793484F610255FC6D1D76D7D9C2B8B5B44A66
SHA-256:	68FDA7AD52EEF8E4F79DF968C87C417114E8B74D19F3FE388EB0BEF6F1204545
SHA-512:	5A9D989C14DD264B9FDD221EED4ACF158ECBCA2D0C6D168FC2DB5370232F45729DDAE050719D82A09B3AE4F82B0779AEB00DA6139FA0652D7056BB18F3A1F3
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="com.adobe.reactor.dataElementCookiesMigrated" value="true" ltime="2494014032" htime="30861858" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\MU6BDC66\www.xbox[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	135

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\MU6BDC66\www.xbox[1].xml	
Entropy (8bit):	4.72482244726982
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsnObemKmlULF0VqHIJR3+VWX69qSRD2LKb:JFK1rUFjgemKm6GVqHIJR3qQ6IDb
MD5:	73720BE80853D995414CEC02A46AF3D5
SHA1:	2C847BD404205BF4BE3C10D968F85B13C9EFF682
SHA-256:	4EDEBBBDBD8F13AA52B226C1A69D6C79234CA4E3EB154A5BC9FED77DC4764ECD
SHA-512:	69FA423F907899CA2FC0AC475A3AB2180599C46112F52E711EE105FEE07C216997B16942D5109C32976EC70C457FB823E47BBA0AB1A65EB5AD47E08D4AF4173A
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="com.adobe.reactor.dataElementCookiesMigrated" value="true" ltime="2577224032" htime="30861858" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{A84CE464-5615-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	63720
Entropy (8bit):	2.150585249289539
Encrypted:	false
SSDEEP:	192:r9ZOZn239WdtwfS9Mw70f+RsrXdPW0jF4DW/arqPwg:rTa23Un+vw76+sX40jS6/a2L
MD5:	12E89F7DEBE1CB557598C4858E3FFED0
SHA1:	EE3C87B98F634E5628957A77F2EC09E9C1A7966B
SHA-256:	7820BFAF494BD135B942254D3E26E33C540E428EE90B2B769D18601E1EDF1EA
SHA-512:	4C2C126D0CCA74FBD81BADFC1EC017DB61531617E48FAFD9B764394D643F1DBE8E606DDBC48AD88FABDAC49B4F5227D2041DA7DA23EDBC8B1B627A21BD1DE5D
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\{A84CE466-5615-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30730
Entropy (8bit):	2.297969533828093
Encrypted:	false
SSDEEP:	192:rDZ0QY6SknFjB2IkWQMvYTTVMdl0o8LzblA:rF9jLnhwMlvWTGdrZLPvG
MD5:	DB05D6F75384E7293E2557ACB6683E2B
SHA1:	1A2AE73712547F701C8464CD96961E47AC29B639
SHA-256:	59999BBAD135C806F6E465DD420DF5F2D21D9A4E4A0FC00DB0171677C89EEF65
SHA-512:	F1AA3623200AA7D9A21EAA3CA0BBCF5ABAD86F84908F7062B1AB72178645136E6CA1C8BF843046BBBBB61F64FFAE1E1512D296CE2166459585B7AD4BDF55D59
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\{A84CE467-5615-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5847462038210012
Encrypted:	false
SSDEEP:	48:lw1KZGcpr7KSGwpaF1G4pQvnGrapbSjrGQpKFG7HpRgsTGlpX2zGApm:rA/ZOaQF6TBSjFA0Tg4Fig
MD5:	9CC660A16EF84331AF49721DB8159D68
SHA1:	3CAB8D35D9CFB784BDD27810757E12F0CEAA0F02
SHA-256:	5675A3D773A1F126D71922D83774FBDB8043A5E949B825921097602142434C45
SHA-512:	DD59241FCC25AAA1A76B26632545037AF74E8205FA4F528CA6085F421266AEB4B9B8F44185E5A55C504CB7C135447B209BA5227F25F667D43E7D280D486702D5
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A84CE467-5615-11EB-90E4-ECF4BB862DED}.dat	
Reputation:	low
Preview:	R.o.o.t. .E.n.t.r. y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{BC5DD018-5615-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	185544
Entropy (8bit):	2.522960555461386
Encrypted:	false
SSDEEP:	3072:hP/rDo5STW0Z1wln\NpRnk3ydNRnkxDzVP:9
MD5:	F2E5605EB6D035DC9081AA521994CF1A
SHA1:	BFFA0C6CDEAABF8A040F920659111B2771A770B2
SHA-256:	FA6376BD730922FD4F73EA8F126ED6254A89AF25B0B689D10113C91E8FFACB7
SHA-512:	83FA0F1262E2A9BD0FD8CB6D6971B248EC066141B993814F90106F92C49F0F6CAB8528EC709635CCF43F8F8C58901230B97ED7CA4A41076C9F97CA6F91D8CCA
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\{C59AC6F3-5615-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5610755588130087
Encrypted:	false
SSDEEP:	48:lwUGcprxGwpaFG4pQJGrabpSTrGQpKQG7HpRMSTGlpG:rlZrQX6pBSTFArTM4A
MD5:	4518A8CAFEB29C1990769CC716C66137
SHA1:	9014DBC00F2263459BA6C109B81C80FF492970CD
SHA-256:	F427C8D9D9D5AA8CEF2CE006C59762352C9616AC04C99E6B3B1C234D267607F3
SHA-512:	D20471D533A2910D772D19970700D311C2B95B1E05C705B1F27EA7D8A80025E642583A44C886C0CB7C87D8DD314E750A543C11839B5768E5107D2ABA4F670A8E
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):	5.0645434388686486
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEwmTfmNCnWiml002EtM3MHdNMNxOEwmTfmNCnWiml00ObVbkEtMb:2d6NxORMjmsSZHKd6NxORMjmsSZ76b
MD5:	673845C8EA61590AA94D72781242DCD0
SHA1:	FD64498E52685345F5F8F6AC5095C650CB72782C
SHA-256:	E6D9754BED84B7C413A10F12696F1620BA9B8A5520F29E73759CD450C1E5B13E
SHA-512:	075C639EFBC275AB9964FD7822DA80C6B2B0A1BD38DD335BEB5D053B3CE5E4980EEAD7537FF38BBB267CE84C36E28F6AFB39B2E076D3C87FD75D48E206CAF259
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x7e70e4dd,0x01d6ea22</date><accdate>0x7e70e4dd,0x01d6ea22</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>0x7e70e4dd,0x01d6ea22</date><accdate>0x7e70e4dd,0x01d6ea22</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):	5.1000191573978295
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kQTCnWiml002EtM3MHdNMNxe2kQaCnWiml000Obkak6EtMb:2d6Nxr2SZHKd6NxrZSZ7Aa7b
MD5:	78100DF01C5EE6E2658EBEE4DA183626
SHA1:	A66CED7EA3A48A312613BBDB6FFD2E05A9D7A485
SHA-256:	8230E25ECF41C651DA46D4754CD3F9EA0311B6E7FB22CDD77BD3E9AF39BC6A96
SHA-512:	6AOC79A19C60EA56E0432D993EE0751F52B5C70C33DA1FC4EBFBA705D59B9EAA42798133698F5FE1A88467CC6F2EE8B0A82FDD41A0F4956749064EE5EA328657
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x7e5dd200,0x01d6ea22</date><accdate>0x7e5dd200,0x01d6ea22</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>0x7e5dd200,0x01d6ea22</date><accdate>0x7e603465,0x01d6ea22</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):	5.11968857570745
Encrypted:	false
SSDEEP:	12:TMHdNMNxxLdQCnWiml002EtM3MHdNMNxxLduCnWiml000ObmZEtMb:2d6NxxvSZHKd6NxxvPSZ7mb
MD5:	EF8FCB95609D387029C6B6B44F18F8C5
SHA1:	07C4ABDF5652899288D9CE2399B82B21D9A1D593
SHA-256:	4637417218130EC6714F8BB37BCCF33DD82FAB8FDC9B0E52776C0654EC31C1D8
SHA-512:	3BF22FD7A582889BEC4A03C244DECC0B1EE775F68085A3DFB82BFD235A9BDB1E4B1FCC97DC1623E6BF674B09BB4D7D2C6FBE77FB96A22330B0B41F36566CAE40
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x7e734721,0x01d6ea22</date><accdate>0x7e734721,0x01d6ea22</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>0x7e734721,0x01d6ea22</date><accdate>0x7e8fe355,0x01d6ea22</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):	5.089977188787304
Encrypted:	false
SSDEEP:	12:TMHdNMNxi/GCnWiml002EtM3MHdNMNxi/GCnWiml000Obd5EtMb:2d6Nx2SZHKd6Nx2SZ7Jjb
MD5:	B898B93E9022822B60075850BD223A96
SHA1:	4B66187E6282CFD7C6E7AFEC3750A02E222EB65F
SHA-256:	45A0E7CC47FF7283AD5D510682EEF4C1CA821FEC1D9869EDC3D34A69204582B1
SHA-512:	3EAB8BD119B7436AFC1CDAABB6723BA6CD2A3AA7F41E7764257911E2D436EB24335B438CFA575063B5FE1E65F3AB3929A932AF29CD47D295AE118AA3ECA24D5AB
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x7e6c2025,0x01d6ea22</date><accdate>0x7e6c2025,0x01d6ea22</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>0x7e6c2025,0x01d6ea22</date><accdate>0x7e6c2025,0x01d6ea22</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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Size (bytes):	656
Entropy (8bit):	5.1231415938627896
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwzuCnWiml002EtM3MHdNMNxhGwzuCnWiml00ObK8075EtMb:2d6NxQwSZHKd6NxQwSZ7YKajb
MD5:	B62123A9F610AEFF2E036BE6D2775CD8
SHA1:	33CF2059E37D788F9C7BEB2F4D715054D2DE6EA5
SHA-256:	A1AC356FF9FCB0DB5BEE6DCC6E0028290846DBEFFEF7E95430100DC2930F4CE0
SHA-512:	A3BF5C2B758B6AB57B5AC099C1401E1D3EC6E9E3817A0CDC065574FE5BB6A7F9579E1FD5E21F949DD116856675183356BB3FD96A141FE7AFEF82E3D0C5B2A9D
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x7e8fe355,0x01d6ea22</date><accdate>0x7e8fe355,0x01d6ea22</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>0x7e8fe355,0x01d6ea22</date><accdate>0x7e8fe355,0x01d6ea22</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.0721202882742515
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n5M6OM2CnWiml002EtM3MHdNMNx0n5M6OM2CnWiml00ObxEtMb:2d6Nx05acSZHKd6Nx05acSZ7nb
MD5:	A5DFD5AC9160CE88B880D2A6C2FA2892
SHA1:	D3484C625F47A2021D7EF96D42B895B3BCED0DE1
SHA-256:	C7C3ACDAA0F97FA944EE00B3F3B4D51B471E4DCA69EEA5450885DC61C77EAFBF
SHA-512:	7D008058B94B172078BBCBF3A120E9D3747675C1BE5F8E59187A7EE2DABB5B1AD72EF9C0026631D9E9D3B68FEEB609AEA34BADD055FFC9510160343374F6C376
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x7e6e826e,0x01d6ea22</date><accdate>0x7e6e826e,0x01d6ea22</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>0x7e6e826e,0x01d6ea22</date><accdate>0x7e6e826e,0x01d6ea22</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):	5.116401967862443
Encrypted:	false
SSDEEP:	12:TMHdNMNx/GCnWiml002EtM3MHdNMNx/OM2CnWiml00ObKq5EtMb:2d6NxXSZHKd6Nx8cSZ7ob
MD5:	1087717CEAEE7F0B21E70CCE09468BDD
SHA1:	3E04652A0D4EA19A3638813610A9D6CF3A88F499
SHA-256:	525FDE2367EC774CA21098D95B7DDEFC1D4C951B54D3CBD8CB6E52A4BC5B3DF5
SHA-512:	747886C55372F55E2FBA5B22319303BE9EE6ADE67BD348749AEE0CF6ACC6ECA2BE7A0F8A94F1E71F2FD641A149884212E39D243D0EC57A9090869FE45F4E7AB
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x7e6c2025,0x01d6ea22</date><accdate>0x7e6c2025,0x01d6ea22</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>0x7e6c2025,0x01d6ea22</date><accdate>0x7e6e826e,0x01d6ea22</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):	5.109022610672076
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\1-WebBrowsing-01[1].png	
SHA-256:	BB88C60C19E587AD0793648DE59E089D35F424ECF0BFF9FD28CF33D16ED1A767
SHA-512:	96F6569C42781418C23B59F7209CF095BA5D54C47572B33B0F04DEA94DA1CD6882A6AF94241B09164CF518D66CC1D7739C834801CD62EBB252E1310C7186C81f
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".@...\$zTxiCreator...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.%l.8.?3.c...l5..UUu]7.....1.x<.....0..q....B.z:...H.... ...<.1.q,*...*L....p.(r.k.<o.IEQ\$.b/....2.`...X.Q..y< .....0EX....c#.....'.Bl...u.....a.l....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.....@..l..Y..n.<!DUUUU... +.KF..Q.....l.....\.....(dA7.[l.)B.0R..g..]m.....

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\1083_Panel01_XMosaic_SingleL_Lina[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):	241841
Entropy (8bit):	7.981774637706077
Encrypted:	false
SSDEEP:	6144:kUkiFeG97jbBWKhHvG2zy/aHwyj4pvXYMV3APkzpPnGXNr3p:N9UKhHvy/LyUpPYcQPMOJZ
MD5:	603CD8A2C70BFADAE6DF8849E8653B23
SHA1:	F5B9AF23F477807EBE4FEF4CE6308FD4C3DB233D
SHA-256:	D38E864012820337927D0C8B55368BEF2EBD67FC789EE449D024B018639335C0
SHA-512:	9A6E3AF494FB49C1B1293D3E7074F4DF513139C93842AC8986D91E5BA20817B75C130D9A621B58AF3BA563761F4F36330FA7E7742DC0C26783A153FDE1995F45
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1083_Panel01_XMosaic_SingleL_Lina.jpg?version=6373cfe6-d4a2-e52f-f0e8-bc5b64699a69
Preview:	JFIF.....s=.6....\$7...1L.K.....B..@Q..0.....&...D.w..>..u.A.>g.ljb.H9.GE.....H.22.....)\$...<D.q..Jld_.....I.\$Q.....&...D.w..<.m@l.l&.^."L8.*e^4.....L...0.....m.,P..\$.Q..Q.....J.&.`.....&&b."z3...m@#Q.....D.....`B.....M<LF.D.g.D.....0.l.....0.)uF...`.....xG.4.....0..\$.<LM.L.x.....X"3.....O...=..h.....J.L.X.\.C.:@.....F.....`..HP"3.....O...=..A4.X.A..M+ ..KK.....\..f.....(.....Df.....Ko...=.d.X.\$.-.-1...9.&p....

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\1083_Panel04_FeatureGroup_Need[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 1083x609, frames 3
Category:	downloaded
Size (bytes):	228028
Entropy (8bit):	7.982439965505789
Encrypted:	false
SSDEEP:	6144:aqbFGp4/QSVCPRYWalU5YuoqH6A3c/hEPThiikbDYO2U:aqbF7HVCZpU5RPeGPTp2D92U
MD5:	36EB2E4866A82DDC9CCB4C15D1A4CE1C
SHA1:	766412A78E7B16C953FACA207CC01011355E4404
SHA-256:	8536B31B32FA0B78FB51DFFCB4D3B82FB06C0B74BF943A163DB8E0E4A350A2FA
SHA-512:	72323BF138ACA9AE5AC571F99F60D3CF47B537EFF22601C0264CF0C724A16A2D1362188211000648ED5EE42964B548826329843116A542D11BAADF68CAB23F97B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1083_Panel04_FeatureGroup_Need.jpg?version=91703ef5-c3b8-2d66-a08c-97c99700ca58
Preview:	Exif..I*.....Ducky.....J.....http://ns.adobe.com/xap/1.0/<?xpacket begin="<?xml:lang="en" id="W5M0MpCehiHzreSzNTczkc9d"><?xmpmeta xmlns:x="adobe:ns:meta/" x:xmpMM:DocumentID="xmp.did:E9A5235D5CD811EA88EEDBD181122FD0" xmpMM:InstanceID="xmp.iid:E9A5235C5CD811EA88EEDBD181122FD0" xmp:CreatorTool="Adobe Photoshop 2020 Macintosh"><xmpMM:DerivedFrom stRef:instanceID="849B4255D84E95FCDEAD1A88F392308E" stRef:documentID="849B4255D84E95FCDEAD1A88F392308E"/></rdf:Description></rdf:RDF></x:xmpmeta><?xpacket end="r"?">....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\1083_Panel05_FeatureGroup_Included[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):	121016
Entropy (8bit):	7.983615378018521
Encrypted:	false
SSDEEP:	3072:6HE0TC4ONnwg4PluyDYS3NKasdN/g4iWIOVTdHruPt:WJW4ONnwgOlbsSAxg4iWlehLu1
MD5:	C6782E4DB8BF7AB5E774AB74803791CB
SHA1:	0BC71F790149552889F8378EAC270225B3A6ED42
SHA-256:	381C9BE9DC18C3461197C203D7B94286D7AF0861FE0098D28DE59B28219B4C44

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\1083_Panel05_FeatureGroup_Included[1].jpg	
SHA-512:	112F09CD3B7BC857CDE1A02F98140F678C02D245FDC6DECA39BAA1FC467F5E435B64A752E307324854E75CE7D9AC707B45054E393D1DE1B9A94348A28AAD042
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1083_Panel05_FeatureGroup_Included.jpg?version=1ead3146-348d-72fe-5d73-67e8a3018347
Preview:	JFIF.....a;.....'.N...2_';F.l.yh..O.z.c.2(..Tlh1.G.Q.....+..AU.\$UQr..U.NoWL.....z.'..o....2.P...B.....oO.()(.).~.....v.....cUZ.....+c..Ez.G...Tj..=Q.S.j...D.?(...?....W2L.....{2%H.8blq...f}:v&..E.....5~..M.Y.....!X.t....F...i+....W...)##..F.U..\$.<..Jk...^I.s....j>L.#.....lqG...{.....%....W.f... ...i.^..bc.W.A...j4Z...F.,s...Z.k.r9.U.G.yo.jz[.ct.&cM.kx...E.m..F...x.G.E... W..Q.b.l..lu..'x....F#\...Z...*...E{J..S.s.j~...U.I.".8{#..N..h.f.i.}.~3J.. ...lcQ.F.....O.#G.-s1...=.....nPH.4...26.d.x....h...Z...n5..G..9.....?k..Q...0e...t.2\...Q..#Z.Y.,....T\.....7.vs..TZER..z...5).L...F...9.H...Z...k.s....&K....\$s."#U.S.y.M.<..l...=..._..._...{[...u.. ..#ccc.'.....=o[...h.w~.q.y..e...{7..v-.

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\1083_Panel06_FeatureGroup_Gaming[1].jpg		
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe	
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1083x609, frames 3	
Category:	downloaded	
Size (bytes):	259454	
Entropy (8bit):	7.991415388003182	
Encrypted:	true	
SSDEEP:	6144:13hnkt5PdPEVzehHrZT4+q97yuuOCWmF/8uA5zz:nnkgqHR9Gb79mFEuoz	
MD5:	B8F0D4F6E846F168B83C83E26B92E873	
SHA1:	083F8E22959D0D9A22BB45D0EA8E641BE77A94EF	
SHA-256:	BF77A38A3560CB4F13CC945B923E2C31B6B47B015296E1819CB29CD8F4A1C007	
SHA-512:	3FB240AC5C766B7BC622DB388C3197F8DC43F93ECB2A8103E6357ECD65F4752CB7E8B98B787C7A0A87618A39594242C281DBA8353C09AB15230D86398A092F3	
Malicious:	false	
Reputation:	low	
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1083_Panel06_FeatureGroup_Gaming.jpg?version=21b8d32f-c6c6-aef3-5a17-1179fd22d7f4	
Preview:	JFIF.....a;.....*N.J<.0..v.D.5!..j.k.....O.Q... .OLF...fi.....S'iz]7uQ.yU*7.O....T.....m...#...0Wem...vl-.....h...A.pl}P.X.1'...'."n.O ".....Y\$L.6`....._Q..%.....F5Z'.....C Y.2N.J.;;...>...lp..OF:Q. .m.z8.O.....b.\...(...9sB:s:N.T.%w...%7.y.P.a.9;<..v{4....h[.~'V<G:..b...t.%].....D.A'.f.(Q. f.Lz.'6...a.....&M...)..Y.....<e..H.....e.G..".C.j..E8.s.).....[T..%tVN.....dO.....N.=1....q V...D.w^u...J.W+...Z..W...m\'.5.....K..@.?B.{...X)-a8...x...z.!...~..r...<5~...M.....V.y.2X~\3rS.J..p..V:X..'z.l.=.'.....lf.9..N'pH...=.....Vd\.....>...W..P..~z@g.H)...[qe...V.(Y...V.BE..56D...n.P.6..l....(<K!.*_J\Da.....Z..G.../p....P:~f.y.... <*.Go...C.p...r..Y..i.;?..k*.....x....G55.	

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\1920_Panel01_XMosaic_SingleL_Lina[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, 950x1072, frames 3
Category:	downloaded
Size (bytes):	192971
Entropy (8bit):	7.981560155202067
Encrypted:	false
SSDEEP:	3072:eMHPbWxQdGg88Qe7RDpdsTaR0r6MuA5MWOq2IUvODsZUdh0E1ECxTIYUp+JDSjghNDMT9ukMWOq2nSrhJ1RDYUp+
MD5:	AF3F6D42AF055A2E3A1FF572378B7AE3
SHA1:	C2EC087DDD30D06900FD22ADE688735487BFC687
SHA-256:	9900CC5CA1C99D45947B69E822A0CAEF85ED54D241FD9ADD75FDCDA88E76A130
SHA-512:	7B6311581FF63413171DBE15C94A7224BE2A0873413D868D6AE714B72B200357F4B666296EA6323B3DC9992203864746C525F947CDC03C5F001491D91816D541
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel01_XMosaic_SingleL_Lina.jpg?version=62faa73f-e14b-9432-b764-2a7cb102f396
Preview:	JFIF.....0.....H(.l.....x..R.l...U..bZh.l&/.....@.....x..R.mF.Y&.A..~{mJM.l.r.=....."P..FF@....."d.l..k..m...BJ.%.....D.F. `.....B}...0..! .Nm..H..X.....`d.....2'E'...V..u.."....W.n:.....@.l..@...../..@.ja.Q.^#R.[.....Z.....&.(...P&..3...\$%...j.....!.....O.3}.2....\$.:..b...f.....)@..F.....K.&Q." .BM.);....4.....0.....&...0@.....x...v;...f..F.H)r.S.....%@...0L.(.L.....e...g.;.Pf...%o..Q.r5A.B.E.....F...D.D.i32.....o%...f.rM...&;D.5SHS..... `4..Lp..L..... .8...X}' .W..J N...l..)6.ZB. h'.....

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\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+IQMUmaviYqMz+aSJ
MD5:	030A9315A92BB58A3586B28B1CB61369
SHA1:	2EAFD5EF91D27E557223F3C06EC94D5099C44FE2
SHA-256:	272E8CE9123E9F1978ADF8E83477481CBB8A346B2202C4F36264C3B399A7543C4
SHA-512:	65B1CDE76DCB2EOCA6C406AAFDCEdCA7915CE486095760CB12F3C64709E3B1471A5D9763D2369AB2F937064382087D4B7CEB05B7205B3782A15409AF1C9BF8F

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\2-PlacesYouGo-01[1].png	
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....!DATx..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...o.d...x.e.....Z.Z..(m.ZcJ...o. P..ws\$.\\`...\$../-y...M...!f.svvvj\\.[.'].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.../J.D.I\$.in.....l...x.as \\z.'..t.....K.Lflt4.Y.u)wc3Msii..l.....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\NetCache\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
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....!DATx..w ...g.l.....Z..W.5.....!p!\$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.>+!..33s.M.....>h.].....u.]....._~...'....+W....Vkw...?....[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.....~OCA..Y.a.....Ow.....y...n...l.(RRR...s...9.s.....7...*...<..S..E.q.=.].j.....?..'5'.....)}.....!..!..1..1.RUI.}"i..P..{...!..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.j}..\$Y.z..&{J....!6..e..`O.f.. y.m...].n }{[OCq.w.7^{\$!^x..

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\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:RqdkxbaidSummUb1W/E3J3M/2f/MhQqil1clRwLl:Rx1aid50Ub1W83M/2chQz6EwU
MD5:	F8D0DC34CB1C64F2FC93033ADF52AAAD
SHA1:	FC23B43FBC2977D9A729EF0661F1B38CB08B1984
SHA-256:	94BD6616569E965BDC4C413CBF8F67EF0FBDfD764648922DA5B0AFCBDCACB13E
SHA-512:	3F946D983C048072B3BE7F5B7C8D5921ABC04579051E355C55E77FF430AC130BE5D010B08D893D91C40C4652F5A39BB8749C75CB47B79FCBD5E88B6181964745
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....._ID...pHYs.....8".@...\$zTXtCreator....sL.OJUpL+I-RpMKKM)..Az..jz....!DATx...g.]y .g N.3U.\$....!...T.....Brl..S .o....&Nr.a.....L..@.L....w.k...3....^..~x1s...9..*"...x.*..!....."X.9)}}_...2?.>..@}.Sy5~c..M..0.h4Z.c...{R.c..Z.....5...P.ST.~{~.....?/.QJW.X!l..O.w..zM..&O.C..^...?m;Ch.gF"..0J..J...!..U.q..4S...Yb...y.P.8....!TSfQ...X.l...9....gb`.H&.Y=..X.V...W.....m.q.{d..Z.\$l.z.e9.Sq....!..655%.H\$bYV.[tF.....^...BH*..o..!..3B..(R.u+1`.PJC.P0.L\$.s...5....T...W...x<...!Tl.\$544Tn".PJ.Eq .R....LU.)....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.rl..(.@.f .B...EQTUJ ^9.\$l....{..>7QOU.P....\$....dv .%. ..i...!9.....[vmA..rcY..Tv..!P.e..] ...l....[.-5...._es....4.a)....X..!..B(si3Ly"..K.....u...p..B..RE:+1`QJ=...l.....g...SE=E&..5.....

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\50-f1e180[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	133618
Entropy (8bit):	5.224613249025047
Encrypted:	false
SSDEEP:	3072:1f/HuFVppxvleJ0i9d1EwgXA9JKi5DCE5n:1f/Hu/FleRxn
MD5:	0405301724624162B6706F1AB465531F
SHA1:	1C034383716BCE493E28BFF0DD2C27F049CC558
SHA-256:	A5DD3C05EFED81BBF60B618C070A7746F030147590EE0EDD74459AC4E53955FD
SHA-512:	9D81E61D3B0AED73F7A64D0344E432AEAAAB057655CFEB040348FA876693E618A434D63727F1E4AA1118276740C7102FD412637B46752665B78EB3C81A53915A
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\50-f1e180[1].js	
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketing/sites-wcus-prod/shell/_scrff/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-c07ea1/29-1ec5a9/23-c64e70/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/79-499886/7e-cda2d3/b2-7087f0/e5-08f1c0/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/50-f1e180?ver=2.0&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("/")&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+=1)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\NetCache\IE\0W10PBUV\539_Panel01_XMosaic_DoubleR_Alfred[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, 539x491, frames 3
Category:	downloaded
Size (bytes):	39888
Entropy (8bit):	7.9824125903299255
Encrypted:	false
SSDEEP:	768:P7+675ZvTqvM96keUcF6f5pjixqT/u5VZli49UN+u9i6v1PIN4NEhd82d:r75ZvuvRkeUcaAgKVyUcyi6RiCDE
MD5:	1FE5A4A6B1707FAF109F26A0AB160F32
SHA1:	A65B4EE632FFEC6CFD7339394EAE3E1237C908D2
SHA-256:	7FEA5B890CB7DB2840AD8847EBAF2C0EB752B5DD46E62701FD03813070EBCBA8
SHA-512:	BDCBD99B576C272ABCEC81A08E4B4CC173A4DB01A3395CB9234A8278D9F0F0E681C74BCB4458735D529794C04903575C8E5122D79DAA6A007D27376748D95E7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/539_Panel01_XMosaic_DoubleR_Alfred.jpg?version=f7f68cc8-8ea1-ce11-135c-512f12f1ec9b
Preview:	JFIF.....KI\$.I&B....U.a.....}.d..s:..e.. ..\$.I.2...2].....q...D(.2.B!\$.S.ob.I\$.L.....U..D@@@.Db.8....E...;Q>_ ^\$.L.).fCZ6.....8..C.E&d....K.2z...\$.d...h.X.....0.8k.\$,...\$.Y.ZVq..I\$.d.&...T.DD..c...(.IXS.t.H.5.,u.\$.\$..LL)..b"."..G..z,..l..s...I\$.d!.d..V0a..`.....E.#a!\$.....I\$.d)LB...b...F..p.....`d.....\..I\$.L)LB.5H.D.6..0..8...%(.;T.....T..\$.I.%1.L./#.....8!...'\$.m^..I.I\$..).Raf.....`#p...Nj.. \$...gn...L.d.l&d.R...S.DD@B0...l..t..\$.gn.V.q!\$.fd.&l.^",1.....P.....?I.....'J.n..6t.l&fjBd.E...#.0..c.....5.....[.l&d.l32R.\$.*.@... ..K.....}aaG.6.\$2!\$.Y).&a.....:.. kM.o1.J....{(Oe.D.f!\$.Y...a.....o...8...7\$.....)5.\$..!al.4.c....",1...~Ny...S...e.mC.z.L.\$P.RH...Q..

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\539_Panel01_XMosaic_DoubleR_Jen[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, 539x491, frames 3
Category:	downloaded
Size (bytes):	65749
Entropy (8bit):	7.988472812950112
Encrypted:	false
SSDEEP:	1536:WbXDcqdl5SXnQ6ivUvaaN5pLBs5NdPmLVzaAggR6gSDILBqyVvwBAs:cp9vUvaa3pLO3dO9R/ZLBqcwBAs
MD5:	A47DF82DFB32B9C23B626D73FA841418
SHA1:	1E93E7A6272964AF6932D0F3B62541788836082F
SHA-256:	8C21C1C75FAADF00FC3C57709EA1AE38210CEB7769F74077D36615E955C38A2F
SHA-512:	02A1F7BA94F6696EDD593A4B23BC15130806DC0D512DAA2463F66A9CC5AC05B3CEE2A3BD72EE13436DCA3A2CD0B3ACA26AE4D217AC66CB8752D5AF6F53AC608
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/539_Panel01_XMosaic_DoubleR_Jen.jpg?version=e534d903-d097-7dff-a205-7e6759277187
Preview:	JFIF.....d.b...8t.l.....ZB&D..P..e)@...YAJ...Ax=-.fo....3bG..n.M.2....".4.DHR..c./....6DW3}.L*.....X...24h....(7d...[...E"...psx.....5m^d.(t...q...r..m...\$.7g..%..J.JD...)H...V.&...-B..=-.....[.l.1>.E.PA.7 SD...x."bP(...[...3.#[...B....c.5.5f.....j.....2f..f.%...X.....x.9rZ.....4...".4#b...4.T.4.5].L.7".d.&A=.....+i'.z...\.I\$.....1l^.....Yez.....a.a....:J.s<.KD.H.)...z. O..J..H...(D.JCK...s....*.FN.;.2.R..l.L...1X.^D.G.=..oN.1<.....i.4.f...~\V...X..K.....D...j4V..i.j...u.V.*..T*...=H(...l..B..].z...t.....p.kR3.=. ..)y.....9[.d.B... .R..../:Um.....k)P..EZ...KY/q.....'...E..L...D/..j.XR....[.qa...g....*..._E...\$..N.....7l

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\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
Category:	downloaded
Size (bytes):	78912
Entropy (8bit):	7.978996167181678
Encrypted:	false
SSDEEP:	1536:uzBh/whJc5DQcy5JX+wBGPhO8+8UtUvjcUCoSu0LL4TgbKfNcKjFT9:uzB9Jc5DQcy+fpO8PLcUgu8PmjFT9
MD5:	2C92ED67778825C64FE7A6A5CC1FA0FD
SHA1:	9915BD644C87EE22E1D0790113D6F7848AB1B4FD
SHA-256:	F9E1B0C44E8E4F5B2C2F7A2061FE415B1F1BDE35FFC8AF58478C55D5599D925B

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUI\6-SigninAndPayment-01[1].png	
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.....l.O....pHYs....."8".@...\$zTtCreator....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\$t.t:ZMQ....W.R...\$......9.i.j.U..z..B8.l.....F...\$<...G/w..il....\<...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..l..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...l..+a..].9iY..B.sk..^..SMj<!.H4....wO..6..7...FE...c..5.....z.`Yv.....)}}.x<.....1.

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUI\8-Windows10andOnlineServices-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
Category:	downloaded
Size (bytes):	76014
Entropy (8bit):	7.9817111618181215
Encrypted:	false
SSDEEP:	1536:zJmxM73PEazh0shB3yPCDYztJZHfcr6kE4HZYpdQPhvMF8UpcnmLFn:8xm7HtJ7yaMzFUAKHZYpdOhvk8VnmLFn
MD5:	39B36FED6CFCE5C30C2BC9286D3CAD37
SHA1:	FDF15DFA297BBEECB2CF8D14B04A74E991267DDE
SHA-256:	D1249AE0E56FF3E23AB86CB3528193213BAEEEBE9916134547A88EABDCD5D7D5
SHA-512:	2D59C2044871D80AABA00660347F8F23D60C3FC0EC21E47CC0E56EE039A0B23F93CB07511DB995532F211E77A6C2DDD803508E1B862F4C82FDCF8FB52FEEAE F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/8-Windows10andOnlineServices-01.png?version=b31f0a34-d7b9-64d0-5651-050ed34c78bf
Preview:	.PNG.....IHDR... ..s.....l.O....pHYs....."8".@...\$zTtCreator....sL.OJUpL+I-RpMKKM.)..Az..jz....IDATx..g...y...S.Su..4.3.....("El(...U.i.....z...tm.Kye[.])."Ml..l0.9.\$r..... ...3=.....k.U.z#.RX..ey..s....d.m.M.B.-...gl...h.O.,....._P,...K.=...3.....}...m...qE.....8Q))=.0gny..z674...>r...f....E.....f....m.f.n[z.....6g.....M.E.....?XXX,... ..D..^Z ..9.&~0w)\$W` ..Wn..q..9.o<s.r..Mg.-d..&Z3...*,...2.....[q8...\$..'.V..M..... ..63..0<x.....Y.g.X.q..s...C.l..R~.-.3`.-2....B..e....x.]EVR.....H,b9Wf.y.haa.8.<{.3.....Wi. <".Nl..p..i...4..4...c?J..rb.....bN!.7.UA.<....<J.9"...u..#_f...V.-x~..9.El%rb..0.....bN3.<Xg2..ol.....H....a.XK..v.....l124.iZ...%yv.Y.OV....b.l..G....U....D..Y...x.`.5oX.....o-. 3.m.c.Fgkg(B.%F....E...z....K0.8.u:G.l...%Z8l.ci....%&!.!....)##...jy.;u.rwG.lf[....x.....B..X_-.G.x..."...E...K'U..8.P....u....1>..U.ZlB.....0S2..c...Q

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUI\ActiveOffers[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):	4829
Entropy (8bit):	5.285188761220722
Encrypted:	false
SSDEEP:	96:NQ04uvCfGz3nIARXuRvUYDuz39/H/gDv5rgQ8w9E/A3vJrMz3jpXUdbvFrsz3g4:yO4ur+ReRTDMHIDGMQ6X4
MD5:	7FE99CE34D90C577E94F715802FF5306
SHA1:	AFE2320B149E73C29C71B773836C26D1289B019D
SHA-256:	CCE416E2B3F1CEDB73B6B2518F024760E4CFD0144E94D6CC40F2D8383A941532
SHA-512:	E6E91CA40810D2B8A4769DF58A888952B1D9603F6F1BA74074ACC33826E7EFFA0E800367F8BAA39CBA7A579DCBD9CDE603AF8B3247D9BD83AD4F756D4FD337 B4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://offertooldataprod.blob.core.windows.net/windowsoffers/ActiveOffers.json
Preview:	[{"OfferID":"697885830","GlobalOfferID":null,"BackgroundColor":null,"Locale":"EN-US","Status":"Active","Approved":true,"StartDate":"2019-11-18","StartTime":"06:00 ","EndDate":"2026-01-01","EndTime":"07:59","Text":"Shop Windows 10 PCs on sale.","CTAText":"SAVE NOW >","CTALink":"https://www.microsoft.com/en-us/sto re/b/shop-all-pcs?IsDeal=true","ArialLabel":"Shop Windows 10 PCs on sale at Microsoft Store","CreatedDate":"2019-11-17T22:16:27.0674569","LastUpdatedBy":"Therese Frare (TEN GUN DESIGN INC)","CreatedByEmail":"v-jand@microsoft.com","LastUpdatedByEmail":"v-tfrare@microsoft.com","ApprovedBy":"v-tfrare@microsoft.co m","Pages":["/lte-tablets-laptops-and-pcs","/compare-windows-10-home-vs-pro","/comprehensive-security","/default.aspx","/view-all-devices","/compare-devices","/ windows-laptops","/gaming-pcs","/desktops-and-all-in-ones","/2-in-1s","/windows-7-end-of-life-support-information","/features","/windows-10-apps","/laptops-for-college-st udents","/4k-laptops","/computers","/continuum","/

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUI\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/7uNp0RvmAf9vDBO3rwx8oAW7Fbbicpoj5:nTgmmNrxNAW7pbi2ojq5
MD5:	F710BE24875D1BD47725BE7B5E86281C
SHA1:	15BC09A3B55B96B7F5BD38D6F499173B294EDE42
SHA-256:	404B1F8A226DFFCF14D55323D8D06FE38A5500B31B7B867FC2EABA5BA5888ACD

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\Enterprise_Trust_Center_32x32[1].png	
SHA-512:	258B5261EB685A15CE114AC0E65392719592CF28BA560A241B3D66CFAEA3AE08D92E0FCA58B0E21053B78AC980F327FB2C9EFA885048CCBB8D35459EF05D39C9
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.I.-..%n.I.....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\user1\AppData\Local\Microsoft\Windows\NetCache\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:	DD197BEF9E8EC8B7C17CDEBDA0712DE0B4FB0D959ED44D1668BC5370518D98D3
SHA-512:	1F1ABFCB4CF6402B08DD36E1CB19824C3F205252C421A91D9452EF72315F4FFFFEEB2ECE45A15011CE8E387833ADF4CC38C3B4F9D415D39B0AE7841EB9D426A
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`.

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\MWFMDL2-Xbox[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):	100898
Entropy (8bit):	6.005625423708649
Encrypted:	false
SSDEEP:	3072:JZoBbFo1PvyUW6HHObtacAtB/Lb/Qxb+2Zy:fnW6HHKta/P/Lb/QxbFZy
MD5:	E6684C39227948E823B36FE249FDF9DF
SHA1:	7080AD6AF58EB68F614EFBA7FEF49B56E9080351
SHA-256:	F61EA31509731E06A931C9DF69B1A4A2EBAD052D7E716A967CC2AE7314F49F09
SHA-512:	B42B43BF7122B78EDACFB7742ECC1E861A92FDDD93430CDFAE2A82F02D88244F16C46B76893A9D9DB9AEC0EF60709BBF754F9A19AED07FE9ABA7268F11B47F38
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.xbox.com/en-US/global-resources/fonts/MWFMDL2-Xbox.css
Preview:	@font-face { font-family: 'MWFMDL2-Xbox'; src: url(data:application/font-woff2;charset=utf-8;base64,d09GMgABAAAAAHvwABAAAAABVrAAAHuNAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAP0ZGVE0cGh4GYACLXAhWCYg/EQgKhNw8hK8GC4NuAAE2AiQDh1gEIAWULAEtJJQyENVvwPJGvm8yt6nVEEI/vr0o3GZDXbdf3fEEZK9g2jXq3UyENgtOzkKZuysns////////z89qYhshbqlXbf/5+OgIKgqRO4uQadQmmSoCEhNCil9xDJarkN8kSTadkTTBljkmzzmgtkoVQXPf3sDYQioKJefIRMSNOB gklrhYhC63QHTUjabzDHuu4ga7npVdMyqVKlryUONU0J+3RLQ6zgbuBMPdbV4aAoSrgbXVjokEaqG96E1W0FWJtv8kGqT3kg0vBE3cByK3QVgLGZWHw0MKT5 LrR+Fad2ytdLDx+Ls+wb0j4q+oZeb67yQ1LSclGkITGLZTupEydmPVvA0IduMIEskBUkpCUQK9oh8cCs5/2CiywNulsDtxB6ud9ytDhksWke+B6wV3CD3bkjqOf8hU110F QCOg4Di81FSGNU92dmhf+QuNtZwaP6Ux4qtPvri6pJlAo1TW/oBZ+X//6nz8o3vcFksW/zlrBxGSNZ6dbLw//P/ec+ST5wBgjPkGYssPFA0WPryLXCv6ohYW6Bb8Ehqq7/8+9m/bk3QhBrCRZCmQZpUjptUk3Bq2GXdhUll5ZORu8KK5bZWwGfqH652v+qVglEwYBAkJJDU7tz5/z6u8egsLuKl+3mCdllwHcgW9HuNqc5XQpJM06haAz98zlfX3CfFL TDDjsA7MQK4Mplh1X+nxOWSzoFohUQqkSwJJAv7afJwBHeh/b+wCE4AMgNWUjUIVUqVXu9kdJs3lbn3dZjKkAmIA7E

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\MWFMDL2[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 15 tables, 1st "OS/2", 37 names, Microsoft, language 0x403, type 2 string, Normaloby
Category:	downloaded
Size (bytes):	20040
Entropy (8bit):	6.19996057371802
Encrypted:	false
SSDEEP:	384:FrnW7NB829nIBLy9oHPGWyFLenP+zQgnZfncO/A/xio:cA2wy9oHhsemzFvcOjo
MD5:	5410C5517F1BBEB51E2D0F43BC6B4309
SHA1:	4ADF2D3A889A8F9D71FAC262297302086A4A03F4
SHA-256:	2F4E38662C0FF2FAB3EB09DCB457CD0778501BFEE4026F6B0D9364ABB05DB46
SHA-512:	E0EF3BCA5CEFA4B6B69CE09FC5295E21A5D151912585AE80703139550BD222EF463CBA856EA7F37E9D8BEF21EEBD7790E3A7D81D580469997A8708B11B00E61ED

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\MWFMDL2[1].ttf	
Malicious:	false
Reputation:	low
IE Cache URL:	http://assets.onestore.ms/cdnfiles/external/mwf/long/v1/v1.25.0/fonts/MWFMDL2.ttf
Preview:	pOS/2JZxh.....`VDMX.^q...\cmap.ph....<...cvt .....*fpgm.....Ygasp.....`....glyfoV..."...l..7.head.k....C(...6hhea.....C`...\$hmtx.F.E.C.....loca.Y....Dt....max p.....El... name..b...E]...post.Q.w..MT... prepx.....Mt.....3.....3.....f.....MS _@...B.....!!"...#.#...\$.\$...%...%&...&'...'...((...)*...+...+...-...-.../.../...0.0...1.1...2.2...3.3...4.4...5.5...6.6...7.7... ...8.8...9.9.....;...;<...<...=...=...>...>...?...?...@...@...A.A...B.B...C.C...D.D...E.E...F.F...G.G...H.H...I.I...J.J...K.K...L.L...M.M...N.N...O.O...P.P...Q.Q...R.R...S.S...T.T...U.U...V.V...W.W...X.X...Y.Y...Z.Z...[[...\...\]]...^...^..._..._...`...`...a.a...b.b...c.c...d.d...e.e...f.f...g.g...h.h...i.i...j.j...k.k...l.l...m.m...n.n...o.o...p.p...q.q...

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\MWFMDL2[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 11480, version 0.0
Category:	downloaded
Size (bytes):	11480
Entropy (8bit):	7.941998534530738
Encrypted:	false
SSDEEP:	192:QNhlPjX236n8/cliy01vRGeJsqVZJZmKgiwEkyaGG1QfPujdl5v9QtAOcAue2HCZ:QnjX23W8UcvRaqVZdgiyRQf2+5v9Q0q
MD5:	5ED659CF5FC777935283BBC8AE7CC19A
SHA1:	A0490A2C4ADDD69A146A3B86C56722F89904B2F6
SHA-256:	31B8037945123706CB78D80D4D762695DF8C0755E9F7412E9961953B375708AE
SHA-512:	FCCBE358427808D44F5CDFCF1B0C5521C793716051A3777AAFDE84288FF531F3E68FBC2C2341BBFA7B495A31628EAB221A1F2BD3B0D2CC9DD7C1D3508FDE472F
Malicious:	false
Reputation:	low
IE Cache URL:	http://assets.onestore.ms/cdnfiles/external/mwf/long/v1/v1.23.1/fonts/MWFMDL2.woff
Preview:	wOFF.....NH.....OS/2...X...H...`JZxhVDMX.....^..qcmaph.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.Ot.&...a.pa.0B.1..F...Q.ha.0F.3.....q.xa.0A.0L.&...l.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...j.na..G.3.....}-a.p@80.....C.a..pD82....c.q..pB81..N...S.i..pF83.....s.y..pA.0l....K.e..pE.2l...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

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\Picchu[1].css	
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):	77352
Entropy (8bit):	5.287116118466487
Encrypted:	false
SSDEEP:	768:k5Dos5gKNfBLNEvT0P+rpZikmo0nzRMWcXCEmQTnRi+:0knifdGxSkmbTmQ0+
MD5:	EA61364BBA3F975CBC7C780BCDFA0459
SHA1:	51F7721489B76379D964BBB6C60D48D75BCAC873
SHA-256:	3856D6CB77EFB03BBA3BD888D6C9B6852D4F0F9C6F245A8158C1D77554C80644
SHA-512:	877690ADE452CE9371605B4E6F93BA7C8555A74AFE55067D093D5D016FA07557A9097FC3E0451D340B1368CC97E9CE44B828EC1D092D7E70F81425AA0FC04A37
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.xbox.com/en-us/global-resources/Picchu-Grid/CSS/Picchu.css
Preview:	/*! picchu.css v0.1 Microsoftdotcom team Github - url coming once ready to make public */a,abbr,acronym,address,applet,article,aside,audio,b,big,blockquote, body,canvas,caption,center,cite,code,dd,del,details,dfn,dl,dt,em,embed,fieldset,figcaption,figure,footer,form,h1,h2,h3,h4,h5,h6,header,hgroup,html,i,iframe,img,ins,kbd,la bel,legend,li,mark,menu,nav,object,ol,output,p,pre,q,ruby,s,samp,section,small,span,strike,strong,sub,summary,table,tbody,td,tfoot,th,thead,time,tr,tt,u,ul,var,video{marg in:0;padding:0;border:0;font-size:100%;vertical-align:baseline}/*! normalize.css v1.1.3 MIT License git.io/normalize */body,figure,form{margin:0}body,p{line-height:1. 5}.mfp-title,pre{word-wrap:break-word}.mfp-arrow,.slick-slider{-webkit-tap-highlight-color:transparent}.clearfix:after,.slick-track:after{clear:both}article,aside,details,figcaptio n,figure,footer,header,hgroup,main,nav,section,summary{display:block}audio,canvas,video{display:inline-block}audio:not([controls]){display:none;height

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\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):	5.307600993212138
Encrypted:	false
SSDEEP:	192:JBvutbhjqco07TGERdoXvL/XL5YxjikGeBf:JF6bhGco0fGEcD/XL5YxjilBf
MD5:	B8F0AA2F13F4E4589612684C0B9F80CD
SHA1:	4480B0CC0036C1882E16EB84EF91BB8D30EC134C
SHA-256:	E08D778FCD029DE4EDE198E4DE3A568ED916A39672D2A22B5B85F440A08F7AD5
SHA-512:	A00E732F66DD991125C9F786583042157DFE8339BC7E54E997D265161953215A87B2E79A9D30E73E262FC55909CD662A653ED3799A23AC725C5BE92B19CBB4
Malicious:	false

C:\Users\user1\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RC579ee48d9ed04155b8299e869af1ac51-source.min[1].js	
SHA-256:	1A06A8B35A6707996E12115D082742DBD242D4A78A26ED56883B5521C151F4E7
SHA-512:	B5653DB4DFFDDAEAC4E147EA61C82396385CEABC986CB99BB9F8607E340EBCEAC66D6597A1619339463D34553F5502EC5A5473C06B745B8539CA056C4E3ED17
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/13167260817d/RC579ee48d9ed04155b8299e869af1ac51-source.min.js
Preview:	<pre>// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/13167260817d/RC579ee48d9ed04155b8299e869af1ac51-source.js`..._sa tellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/13167260817d/RC579ee48d9ed04155b8299e869af1ac51-source.min.js', 'null! ==window.wdgtagging&&null!=window.wdgtagging.jsll&&function(a,e,g,t){var n,i,w={appld:'\`Windows\`,version:'\`4\`,coreData:{env:a.getData('\`env\`'),market:a.getData ('\`langLoc\`'),pageName:a.getData('\`gpn\`'),pageType:a.getData('\`pageType\`')}};(!\`undefined\`!=typeof isUserSignedIn&&\`1\`===isUserSignedIn t('\`.msame_TxtTrunc. msame_Drop_active_name\`).length)&&(w.isLoggedIn=!0),w.prePageView=(n=a,i=g,function(){i.setMetaTag('\`awa-env\`,n.getData('\`env\`'),i.setMetaTag('\`awa-market\`, n.getData('\`langLoc\`'),i.setMetaTag('\`awa-pageName\`,n.getData('\`gpn\`'),i.setMetaTag('\`awa-pageType\`,n.getData('\`pageType\`')))).e.load(w)}(window.wdgtagging, window.wdgtagging.jsll>window.wdgtagging.util>window.jQuery)</pre>

C:\Users\user1\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):	5.3361765744156395
Encrypted:	false
SSDEEP:	192:dB53+u1vwkOIOU574BraYQNRmDzB3Jf1jZ6x8br8bWHcGdXG84HQMqhuG:df+hkOI5791UDzB3JhjZ6x8br8bWHcG9
MD5:	56683AE549A7BD9A8067BBB7BBA1DA83
SHA1:	E227A40DDB85B3637E32C96C249102AC4E5ED4F6
SHA-256:	DFB09E0C67853F6F6F720627AAEDE3B1D36B7EAF25AE4121F3391A9F9160A790
SHA-512:	BA9316BA0BBF2ECFEAB92328ADB9649D554B15AC822C7F5B78AAE4F55DFC5C26BE899C4C824EB0D47B5957D0D3A436F278504C2EBBE87D1128373B9957DA1D9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/13167260817d/RC5f812135e64f48ad85ea100034bc60a2-source.min.js
Preview:	<pre>// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/13167260817d/RC5f812135e64f48ad85ea100034bc60a2-source.js`..._sa tellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/13167260817d/RC5f812135e64f48ad85ea100034bc60a2-source.min.js', 'null! ==window.wdgtagging&&null!=window.wdgtagging.jsll&&function(t,e,w,f){window.location.pathname;var m=window.location.href;w.wdgVideoTagging=11,w.video TaggingInit=function(){var g=awa.ct.captureContentPageAction;w.wdgAttachedEvent={},w.wdgVideoName={},awa.ct.captureContentPageAction=function(o){if(23 9<o.behavior&&o.behavior<253&&240!=o.behavior&&250!=o.behavior&&251!=o.behavior);else if(253==o.behavior)g(o);else if(240==o.behavior){var i=o.contentTags.vidid ,d=o.contentTags.vidnm,c=!1,r=(f('\`c-video-player > .f-core-player\`).find('\`video\`');r.length&&r.each(function(t){var e=this,a=f(e).closest('\`c-video-player\`).attr('\`data- player-data\`'),n="\`";(a=JSON.parse(a)).metadata&&a.metadata.video</pre>

C:\Users\user1\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):	5.368535019325185
Encrypted:	false
SSDEEP:	48:DaJt/BuakmTcmF8j4cELIGCnSwndSRoSniNcmF6RFuiWW/04AvDR/YGH:IBB5LS5zi9RZWW//EZ
MD5:	AA99FDB092B9F80869E4581C7CC6DD88
SHA1:	30BCE960A842584E5F61DEA4DCB4DB3EE87A81A7
SHA-256:	CDD05EAFD2C8A31669EB0F910FDF43D595120BBC3350C9910B08E93267658D61
SHA-512:	F6401E98375ESCf439BFB69E5AEA13AB779F27A058A17B3DF16950AD21CEB9477DD0456878EB80F109B72CEE68C0016A88C4D636FEED073708C6AC47B8394D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/13167260817d/RC95d5954deda24aa780e2bd87a6eabf8f-source.min.js
Preview:	<pre>// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/13167260817d/RC95d5954deda24aa780e2bd87a6eabf8f-source.js`..._sa tellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/13167260817d/RC95d5954deda24aa780e2bd87a6eabf8f-source.min.js', 'null! ==window.wdgtagging&&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 \`\",content_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\`'),ct a:e.cta  jQuery.trim(t.text())  t.attr('\`data-bi-name\`')  \`\"};d.trackEvent('\`trackSingle\`,d.globalpixelId,\`AddToCart\`,n)}jQuery('\`meta[name=MscomContentLocale]\`'). attr('\`content\`');d.globalpixelId="\`1770559986549030\`,d.init(d.globalpixelId);var r={content_name:n.getData('\`gpn\`') \`\",market_name:n.getData('\`loc\`')  \`\",lang_loca le:n.getDa</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RCc17a59b7b91644d889a1351d6aa1b24b-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):	9319
Entropy (8bit):	5.22469742339668

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\RCc17a59b7b91644d889a1351d6aa1b24b-source.min[1].js	
Encrypted:	false
SSDEEP:	192:LBRvprGN7/gQ/1Mh/WwV1rMT9DRQ/1srbOqVwP2+PneINVWY2:L7hrGN7d4/WwV1rMT5uEbJ5+3VVY2
MD5:	06B046B75486BC747362E4743707B8DF
SHA1:	679FEE8982E680720B5B51EEE18E25812E610072
SHA-256:	F1C2FE4FEC72BCE8A79AA8CFB24D195EDBF15E5E2D5CDA95615190EE4EA6E24C
SHA-512:	29732E3A61AFAC0CEF635268582FD81C8B572B9FF5A01054586D0E260E29E48AD8A54CAE64335B7DA7275C0C4C00715DD7505F08DD20808EC8AD562F0A8260D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/80899f83bd8d/2523a52d8f82/RCc17a59b7b91644d889a1351d6aa1b24b-source.min.js
Preview:	<pre>// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/80899f83bd8d/2523a52d8f82/RCc17a59b7b91644d889a1351d6aa1b24b-source.js`.._sa tellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/80899f83bd8d/2523a52d8f82/RCc17a59b7b91644d889a1351d6aa1b24b-source.min.js', 'null! ==window.wdgtagging&&null!=window.wdgtagging.jsll&&function(t,i,c,w){window.location.pathname,window.location.href,c.vList={},c.changeAppld='\"JS:XboxWeb\"',c.vi deoAPI=!0,c.iframeVideoTaggingConstructor=function(t,i,e,a,o){c.vList[t]={},c.vList.inLightBox=!0,c.vList[t].videoName=i,c.vList[t].isEnded=!1,c.vList[t].isMuted=o \"\", c.vList[t].isloop='\"',c.vList[t].shouldCapture=!0,c.vList[t].paused=!1,c.vList[t].lastSentPercentage=-1,c.vList[t].started=!0,c.vList[t].completed=!1,c.vList[t].myTimeSt amp=Math.floor(Date.now()/1e3),c.vList[t].wdgVideoObject={},c.vList[t].wdgVideoObject.behavior='\"',c.vList[t].wdgVideoObject.actionType=e \"\",c.vList[t].wdgV ideoObject.contentTags={},c.vList[t].wdg</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\RCd898c8a8376b41f88f24c93b8645f178-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):	9256
Entropy (8bit):	5.229491069897488
Encrypted:	false
SSDEEP:	192:nB5sDMQCvC7mllmRvu19KFd4nRYw85glFn3K6dN0iX+3x+oS+y+p6:nwMjllmgZRJN0w
MD5:	B145DA069A08E3BA71A0B9DE40C90954
SHA1:	37BE82FA70A19BC533A3247B9A0CB4CC692ECACF
SHA-256:	F79851E68811106CE80F72F6FBA789BB7B771BC6CB69C9E7F5BE064E6CB11C5F
SHA-512:	D59A60E33910B342E9DF10510EEB6F6F2120F1530EFBD30D0DB6E8AFBE7B4C0C64F450A8FD5020A383C6E67428B7669E9EE31747536FBCDE4A0C8139A145DE4A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/13167260817d/RCd898c8a8376b41f88f24c93b8645f178-source.min.js
Preview:	<pre>// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/13167260817d/RCd898c8a8376b41f88f24c93b8645f178-source.js`.._sa tellite.__registerScript('https://assets.adobedtm.com/5ef092d1efb5/e6b4ca74378c/13167260817d/RCd898c8a8376b41f88f24c93b8645f178-source.min.js', 'null! ==window.wdgtagging&&null!=window.wdgtagging.jsll&&function(e,r,u){r.lineage={main_sel:'MAIN',zone_id:'a3',sec_custom_sel:'\",grp_custom_sel:'\",pnl_custom _sel:'\",subpnl_custom_sel:'\",exclude_sec_sel:'\",after_sec_tag:!1,after_grp_tag:!1,after_pnl_tag:!1,after_subpnl_tag:!1},u.isDebug=!1,r.lineageSetupCounter=1,\"1\"== =u.readCookie(\"debug\")?u.isDebug=u.readCookie(\"debug\"):-1<location.search.indexOf(\"debug=1\")&&(u.isDebug=!0),u.lineageDebug=function(e){u.isDebu g&&console.log(e)},u.lineageDebug(\"JSLL Core Lineage Start!\"),u.getLineageName=function(e,a){return e.attr(\"data-lineage-name\") e.attr(\"data-productid\") e.attr(\"d ata-sku\") e.attr(\"data-bigid\") e.attr(\"data-</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\RCfd46e863449c4326b49b6f8f0201afc1-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):	5834
Entropy (8bit):	5.366394013646339
Encrypted:	false
SSDEEP:	96:zBBv9azUi4Lr8WB0r0/L9W3NVKFFgE5AzaiN/FgPVKF8gJ2IZt/FssgVKFvsDbIK:zBV9Fi4Lr8e0r0/LY3dRzZN/GwQIZt/s
MD5:	E7D84EC934B9DF5CCEAB335014D1AE86
SHA1:	DC4B105B15B2C791CDFF635071AA43B90D49B314
SHA-256:	024FFB4FC8D616347FCDA50139CCC7471FEBE79BFAF5F252C41D69813E4272FD
SHA-512:	5A89B7ECA593D287A26B5F91F485A1CA157474242450AAC39880AE072E45B0FB620483BAC74858768580C3BBF0985B8FEDAE33E245CF6B00FE27B5558FCC0774
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/5ef092d1efb5/80899f83bd8d/2523a52d8f82/RCfd46e863449c4326b49b6f8f0201afc1-source.min.js
Preview:	<pre>// For license information, see `https://assets.adobedtm.com/5ef092d1efb5/80899f83bd8d/2523a52d8f82/RCfd46e863449c4326b49b6f8f0201afc1-source.js`.._satellite. registerScript('https://assets.adobedtm.com/5ef092d1efb5/80899f83bd8d/2523a52d8f82/RCfd46e863449c4326b49b6f8f0201afc1-source.min.js', 'null!=window.wd gtagging&&null!=window.wdgtagging.dcm&&function(e,s,n,g){var t=function(){var e=window.location.pathname,t=window.location.hostname;try{if(n.addToCartSelectors= ['\"button[data-bi-bhvr=PARTNERREFERRAL]\",'\"a[data-bi-bhvr=PARTNERREFERRAL]\",'\"[data-js-href][data-bi-bhvr=PARTNERREFERRAL]:not(.f-precise-click)\",'\"a[h ref*=microsoftstore]:not(#headerArea a)\",'\"a[href*=microsoft.com]\",'\"a[href*=/store]:not(#headerArea a)\",'\"a[data-retailer][data-retailer=]\",'\".sku-chooser__panel [data- xbbigid][onclick*=OpenWithExp]\",'\".sku-chooser__panel [onclick*=OpenWithExp].xbstorebuy\",'\"a[onclick*=xboxContextualStore]\",n.addToCartSelectors=n.addToCar tSelectors.join(),e.match(/\\</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\RCff3b108562df43d6ad12cfb6aac1c005-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\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\RE4qVml[1].png	
Category:	downloaded
Size (bytes):	798
Entropy (8bit):	7.254306261695335
Encrypted:	false
SSDEEP:	24:mn5dFLfeSEHmJXBu5EK9eZtAiBLkYv9i0sklp6k1:m5flfeSEHmZByElsDoY4BklL
MD5:	E3660BB509E9D3C48226346DA365E316
SHA1:	E00526C27E167E370D9C9B793DE0CB779BC2A586
SHA-256:	69403E9DC76021DC89D84FC67D849227FFA72AB2312F04A56EE41DF28FFAE956
SHA-512:	C57094782A7787478A04C0BEE953B5AC08C71A48D652083B0D4211BB294F0C2D9E496E09F7CE5C7EBE8DDCB467FBC6C489B06017DF8DE6DD7105BCDBC20E2B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4qVml?ver=3f68&q=90&h=40&b=%23FFFFFFFF&aim=true
Preview:	.PNG.....IHDR...'.(.....J+...../PLTE.....U.m.. [g.f.r.j.r.g..R..R.w..S..t.V..u..x..v..v..V.....u..v..Y..Z..u..x..w..w..x..v.e..lIl3..h..---DDD9..i.???>...w..x..t..{.y.i.....111FFF.....&...x..CCC.....-.V....333...../.....a..x...//.9.^...atRNS..`....T....@L.....x.....L.....v.....L.G....orNT...w.....sRGB.....#IDAT8...N.@...@..Z.X..ou.]...j...umq.....A.....<.....O4.....z4.4..6.lq.Et.E.h.H.jz..A..v?....w...KL.&..5....S..j.....u.u...."#..F...:..u.uR...6Msf...g.p]D].IY..*Y[g.....;Lw.P.Q.2...\$wD..pRpO../....[....}.7.n..B.*???.#.>.)P*.9Gn.#..j.sM..".j..a...?Jv./7ML"....v.B.B.Oj....IEND.B`.

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\RE4qVmr[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 38 x 40, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	634
Entropy (8bit):	6.89790447108351
Encrypted:	false
SSDEEP:	12:6v77QKACBusi83FnKlf6TkOi25i2XubcHs0B34RKbHiUj2;jZusigKe6T19Y2EZloQHK
MD5:	05F87E0284A2FF3E5FFE91B410BFA4B6
SHA1:	B0332DF2B74D6407222AB75393969C35B46C70A2
SHA-256:	6CBD7B13F6DCFD909A22020C21A3542EADD322F77C6ACC7423E58C5A58E0FC55
SHA-512:	985294D6230391CF7D823AD20A8C6176795871D71A4272FF7C8BBF658F3F63DB6BB1072D972A15E09881059D0C38D373BCC41A5612E726B7CA17086DB6B82FA8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4qVmr?ver=bafb&q=90&h=40&b=%23FFFFFFFF&aim=true
Preview:	.PNG.....IHDR...&...(.....x.....PLTE.....zzz.....111....._XXX.....CCC.....222KKK.....x..v..v..y..x.....//.x..-.....?tRNS.....oW@.08..a...`Q..!.....;.....5.?...zJ....orNT..w.....sRGB.....IDAT8..ko.0....Ve.NQ<yNE.a....?Y..2+d...J.;P.9.[q.....)....)....paeK%F..P..3...[.G+..FQ....!#Z.....Y.....Ev...M...".R.-~v.\$..y^..I.T.1...""...c...X..q]..Y..Mpd7Z..K.z.{.k.+..X)x0.....eOy.l/].^.-.....!.....e.....6...[.F....9...RBCV<...?4....?....IEND.B`.

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\RE4qZpg[1].wdp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG-XR
Category:	downloaded
Size (bytes):	18711
Entropy (8bit):	7.879125720338833
Encrypted:	false
SSDEEP:	384:e+KlooflhrVvMaESGZM0JXgOCrYX81Gx8l/x9AoQYJNZ:e+KoNhr61Sy348xn/36Af
MD5:	996AF36AF03A6BFB1654B69FC907A31B
SHA1:	1724A4F1DF9BFD5426111A0C2A7699EC52E549C6
SHA-256:	1CF63BEC6AC27FB198DEB2DB704602465A5AFCCE262F17C3F656D0FC1F0C37B
SHA-512:	8CE3C41F2FAFF99441A2374447B2091EB35E91239CB5D59C2D6EC1775037CC57BD0839FB5AD41FF32AFE11A3BBA3CEC9872765FCFCFCFEFA0BFA62F719B5E851A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4qZpg?ver=06c1&q=90&m=6&h=180&w=321&b=%23FFFFFFFF&l=f&o=t&aim=true
Preview:	Il... ..\$..o.N.K..=wv.....A.....\$.B.....\$.B.....H.....WMPHOTO..E.q.@..0...;8B... ..;9h..... P.T....0`!...k.9"Jw..).iX`0+.~.lru.2.k..1.9..0 nk...J].j.6...6l...R.9^...W...S...x... .j..3..3.v.b.....K.4...M...-!..E.U.....u.Yk./N.(.....x.....Q...v.....!...2b7&"....(l>w.[L....%l.6.....T&.....G...v.&...&..-aE"...2.\$S..M.tn...u"!f..e.^....8.(\\H.....H)..q.O.l.M\$K[]:}.i..w\$(.S..#J8:=%p#@vo/..P..c..\$.8.Z....!Y'....`H.E.....Pu..l..B.../Uu.....&..!E..l*.(.E7...2*.../+@il.G.#.Q...?&.).Hd...+Z7...\\d..+&U]...v..R(u...A!..ZI.....Fg.l..M  ...#~..`p...4F..MNF.R....kB#..d.\$l.2.....#.nc.@...Y.4...`...Z.l@... @...q..B@...{...@^rqQ.M...C.z.l)S...H..E..Gh...P2f..p<.5H..g.Q.l.s`V5\$!))...Fcc.K...*r...C.l.Pt.+P.T.LC...H..A...5.w.l..4.....5\\.S.E!B8;.+h...B.P?....7...\\.....~ .O).CtX.P.M.j..(.c1]\\.....iX.....T.c.o.o.@..\$f..2.@g

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\RE4r1Ep[1].wdp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG-XR
Category:	downloaded
Size (bytes):	18912
Entropy (8bit):	7.875288835593548

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\RE4r1Ep[1].wdp	
Encrypted:	false
SSDEEP:	384:DY2QLzc9Rfvtc0CqhgfAOfcdAHGmGBJyJGDg/bygZ2e2dO3vf:02QcTcAyRFcdAmmQyJGDmyndS
MD5:	27D045ADF361EC7B7D5C536F3B8B2BCD
SHA1:	23FB7857805CC1901605B6F7E2FD49AC8FFFD015
SHA-256:	AD9834DD7E2580623DD3671171F7A9B8EA034BD3B0F201CBA586C251BB677337
SHA-512:	483EA397343993DCED1FCA62BBB8AABDA4CDA0E8880135FD6432C9D8BE6B2F1E0BCF3380AEC924A7B81809426C49CB3654CFDE0DD7D56CC4AA5E4A1B997DB5E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4r1Ep?ver=4ccc&q=90&m=6&h=180&w=321&b=%23FFFFFF&l=f&o=t&aim=true
Preview:	Il... ..o.N.K..=ww.....A.....\$.B.....\$.B.....ZI.....WMPHOTO..E.q.@..0..d..FHP.. ..<.....0.H=o...v.V.n_h...n.O.j.9g.Z#.2e..C.S.O.....%0a..Yn..m...o=_4q!2d.F...l.2P..f~.D.....b(o).>..UF...4....} .n.p.l.;...G.z.)..r.....@..^l.....l.>\$N.T...G....P.i.1f....vs\$.F..B...DL.Ho..P...5PL.GW.(...fk.....,...x.t.Q)f..z..L....U.H....,+nE..d1O!...j.A.H%mq.....1Ku..7[br.IV..d..aD1.....d.^.....F:d.J..8.3^B+...../.&.....D!...C(Z....Zi....L`N...OVm>...88A2..).T^3..J..g...HJ.jQ..dMW2.la.w...pJ.Gi.b:....+2.Q.U...mSo.....f.....<Y.X....UKIL...Y.#..0<W..IMN....Z.L\zS...i.....d.5`.O.\$25P.#u.C3.Vo*#.c.> .J.K..D..@h....(-(.....)(-...BT.>rX.K.....B.-Th..i..n5..r..> .SjK...k...!f!.....R.M.NQ.<O.\$h...o.....d`.0.0@.r..8.p..L..8A...ii.2....u.j.hV.f.(U.....d...^2....DoD.FLN..k.J`..\$.Sl.L.6...!;.....>r..

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\RE4r3A9[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 45 x 40, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	683
Entropy (8bit):	6.7087910799289485
Encrypted:	false
SSDEEP:	12:6v/7nUBHaWisdlW0pg0JWjyZWqCAL5NBnCa8ml53geyydrmlW6R:XBHakbpbsjEgALTBBHOypmlW6R
MD5:	BBF403C1E0382CD8D9FCEB4B54DFA8C1
SHA1:	91A59140E50C02DC44F00F82FE82E57A99E50660
SHA-256:	60EF459C76A948EE7BD8D8C481D88789332407882649EE4FC5F3A927AFF3B7E3
SHA-512:	76B2585CBBC1BB051F191B2DE13B59BC095F084601EF8FCD2D0DD4F09F41BDB79545938C7C5B023330A1DBC7DD6C17FFAB005F88EE1EF7309D3FFBB0F33D013D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4r3A9?ver=e442&q=90&h=40&b=%23FFFFFF&aim=true
Preview:	.PNG.....IHDR...0... (.....).....PLTE....y..x..x..t.....v..x..v..w..q..x..w..v..v..u..w..y..y..v..v..v..w..o..v..x..w..v....w..w..v..x..y..v..v..w....w..v....v..v..x..u..x..w..x..m..w..x..x..v..w..w..z..w..x.....444.....X.....StRNS.....t...L.G%`. (.c>....e.b...*.B....'.&...}.> .". ..`5\.....orNT..w....sRGB.....IDAT8.c`.....Y....l.....\D).....^>*@...AH8..D.....H..KH.#.)i.l.e!..r..h@A...X.....yTIQ.....Z....`M-\$:.....T...d0a`h..T+#`.L.01e`03'.X0'.XZ.....mB....Qmg...!!NNN. ...0.....e.....0O.j.p..jo..._U...V.....D..FU.Wu`..@U...x.0.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\RE4r3Ax[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 48 x 40, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1214
Entropy (8bit):	6.829513933875872
Encrypted:	false
SSDEEP:	24:dPVdp5Kx/9Nv4SWaT6uZJRSgCv05MhUKulz:vdgr/HTpE/w+hUKg
MD5:	284E9084FD76B7BAD9D3CE65C000552B
SHA1:	DDDC1E2F90A3A607ADDB719887FC256165D85159
SHA-256:	5DFB44F26A66B295CB032AC0C192013F15386C1C8A5B65F77C45A09FB4A0ACD7
SHA-512:	B07597951786D6D6F52FD7FC77F3C777612B14AAF82D8DC442AB61D2138CCBA6BF98BDCA08FC0E551A2ACD12A4CF40538DA0CADABD2CE0A393426EBB256C4E6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4r3Ax?ver=2f9b&q=90&h=40&b=%23FFFFFF&aim=true
Preview:	.PNG.....IHDR...0... (.....Y.C....PLTE.....000...000...--..333.....555.../.....888...../.....000???/.....666...---***---/...r.U..v.../.../...r.v.333-----w..w....w.--/---/.....000.../...x..u...tRNS.H.7G7F.6F.5E..4D.3C....2B.1A.0...-...*.@...'.\$.1...!.. [v...E..t.....s.+.....p.....o.....n..~...m]...c..P...d.S..x.T..e..Ufg.Vh.U..9....orNT..w....sRGB.....IDAT8.c`.....Y....Ls....H...S.....\s../..j.s.> .s..la.E*.Q1..%.Z...R.2H.e...R..P.Js..R.. *s..R.\$jPS...X....?h..l[G..Hs....Pnhd..T..z..l.R..."....+k.X....jX.X..%....u{4-V.....suC.b..V...E..<_?.._3..<0(.....EC.y.""@".1@-q.`!...@\$

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\RE4r4UB[1].wdp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG-XR
Category:	downloaded
Size (bytes):	13647
Entropy (8bit):	7.890884890440031

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\ScriptResource[1].js	
Size (bytes):	26954
Entropy (8bit):	4.516288580103467
Encrypted:	false
SSDEEP:	384:EMgviMjM4if38GmhXeC1QRwweTkBE9wbOY4Jf/JhRZ5h+73hNvt8oC4veONhLYVi:ZLEiJSdo11viYHqb5Klo8v
MD5:	3DBD97A205B8CE59D755AB94F8C42964
SHA1:	B0520226342BBA131160A510BA3B57A1E8B7B80C
SHA-256:	36F7B9FE80A026A5D933855DE494AC6B7A4D01A93C26CE8A8737EED0C79367F4
SHA-512:	82BE6F1015CC346811EB736BD78F4949C855E49F8B4CC8493B22AE0F8D329EFA34205599E1138E57D33302B8A7B76F085DED053530B0F79D0DC71E257C99D80C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cmrinsure-my.sharepoint.com/ScriptResource.axd?d=clUfelLllpVJe0ra_eq80vJ2bC2Z2x5DSGiy1HHlOpLsB3TbT7B_amVBapRUBr7J_tcdfR071le-AtUnKfDu7zkoUcfSAypCyNz613qClq6mHDKv8dxmiFOOgOH9LB.JtHObekBtvUH3pz9llvA5PJLgbeYcDB9so3475Nrsl41&t=58ba508e
Preview:	<pre>.var Page_ValidationVer = "125";..var Page_IsValid = true;..var Page_BlockSubmit = false;..var Page_InvalidControlToBeFocused = null;..var Page_TextTypes = /^(t ext password file search tel url email number range color datetime date month week time datetime-local)\$/;..function ValidatorUpdateDisplay(val) {.. if (typeof(val.display) == "string") {.. if (val.display == "None") {.. return;.. }.. if (val.display == "Dynamic") {.. val.style.display = val.isvalid ? "none" : "inline";.. return;.. }.. if ((navigator.userAgent.indexOf("Mac") > -1) &&.. (navigator.userAgent.indexOf("MSIE") > -1)) {.. val.style.display = "inline";.. }.. va l.style.visibility = val.isvalid ? "hidden" : "visible";..}.function ValidatorUpdateIsValid() {.. Page_IsValid = AllValidatorsValid(Page_Validators);..}.function AllValidators Valid(validators) {.. if ((typeof(validators) != "undefined") && (validators != null))</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\ScriptResource[2].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):	40329
Entropy (8bit):	5.24641079736423
Encrypted:	false
SSDEEP:	384:ovrc3TrJ1vMZCKZ4LpRy6DkfDLcbTzcXanT2rx64aKqR1vySAwBaPUge6yde:oTaYB4Hy7mTzcaTKStrwSAwBaPUTdE
MD5:	AECA88483779AC14B47F14389139050F
SHA1:	B2D6ADDFD778216B8577A9788144F6313900B05E
SHA-256:	38DEAF33D1C84196E4C4F3C76C67587090CF261D423B9BEF9BADF535BC146A2F
SHA-512:	31E647B1ED341AD85DB4E991008F3A79169CCC0DC68E63DA0F0533E1F9875B871336B5B5C953B267AE4788F0ADFCE6F54E3492C4FEB8E087021AB84258F16BE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cmrinsure-my.sharepoint.com/ScriptResource.axd?d=ysbTTiSZxTLNI-aW6sA9VsvqwD3-4n_DuZLVoliY5DXorm4bQBSexHKaRiBHAhJiQkn3isrcE6XB35rGTsae58S_0gb8naR08far14pof4Vzp73v22yWye7N-3_Ae-SJukyA_4a1Og20uZoEt6gvrLiIFkdSfEB8V5k_AW8aCIf5dmygtQZhr6CQGsl7fpss0&t=4f7d5f1
Preview:	<pre>..//-----..// Copyright (C) Microsoft Corporation. All rights reserved...//-----..// MicrosoftAjaxWeb s.js..Type._registerScript("MicrosoftAjaxWebForms.js","MicrosoftAjaxCore.js","MicrosoftAjaxSerialization.js","MicrosoftAjaxNetwork.js","MicrosoftAjaxComponentM odel.js");Type.registerNamespace("Sys.WebForms");Sys.WebForms.BeginRequestEventArgs=function(c,b,a){Sys.WebForms.BeginRequestEventArgs.initializeBase (this);this._request=c;this._postBackElement=b;this._updatePanelsToUpdate=a};Sys.WebForms.BeginRequestEventArgs.prototype={get_postBackElement:function() {return this._postBackElement},get_request:function(){return this._request},get_updatePanelsToUpdate:function(){return this._updatePanelsToUpdate?Array.clone (this._updatePanelsToUpdate):[]}};Sys.WebForms.BeginRequestEventArgs.registerClass("Sys.WebForms.BeginRequestEventArgs",Sys.EventArgs);Sys.WebForms.En dRequestEventArgs=</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\SegoePro-Black[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):	125464
Entropy (8bit):	6.005747342459591
Encrypted:	false
SSDEEP:	3072:1gZ0lpUfn89f7zQV1XrXtISFDnrcqFxcg4qr81/+zShv4uu:pOknlgDXr9IALgqFX1/+Ohv4uu
MD5:	1970BFEAE2E945AD818D3BD5F166DEE7
SHA1:	B69A02687FAE164033DB12D3C4C908157DF09CE3
SHA-256:	E40CC7890C76AAE8DB25F13A77B9A239CB731D06BBF95B3949DE070B38E972F6
SHA-512:	066784D07C899E540E95FC81B60D24DAB881D3EA277EA9622F077B4A28323F29D9F43ABE582C4BDA69032A223143117C393050A998A684947E2FEF33107540B86
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.xbox.com/en-US/global-resources/fonts/SegoePro-Black.css
Preview:	<pre>@font-face { font-family: 'SegoeProBlack';. src: url(data:application/font-woff2;charset=utf-8;base64,d09GMgABAAAAAJ2cABIAAAABeIQAAJ0wAAEAAAAA AAAAAAAAAAAAAAAAAAAAAP0ZGVEOcGh4bgZpyHIYwBmAiQ4IgUJjzQREaQD1TIDIEiLiKIAATYCJAOVAAQgBZFUB6ddDIllyW45RcQa36Syk6Hc7gGd/6 +9QDm2o3Qh2mpUov/XFh3BYeMAGL8PzNn///+//pnEmF4OvCR5+FIKWqtK67oNYu7hYbOqJWqaW2vNFDIz0SpLMXt1LwXeCsplqndf62PbJjRBYrvoHE4IKrHI7CQcbi+ fptH1zK7+xtZ3dnNnLrZ2TjOfcMrLkXVqMQEMUFMEBO8bOK++1C/u7mFK66VyJQqMaXJx25u++VwdhD5IzuXQJz+GyOZF76GF1aC1ICO8u4vJaD0QPMj0dBS eZTRCPNiKRs7s2DuCid9PZfrAVUc3zr81OFFCGo23TVK3losjQhJ+8DKBsEqZ2x94yv5C/IXB9M+4JvucCal6QSW20OTY34dc9XW0Ub75c59WPEujeEncPFX2syp9+YzH sMbFdeYwf/9Z+7OttGXgbHL0EQbseLEC0Xt91j37Ab4hUmiS0UBkAJUiY5CcKQQFaiFdmTuhDmJP2+A3NapuCbIXLhwoBtUQBREIoCggLgnjrlyZe4MLd2NrVnbcjXNrkY tb1O/7+H+G3+fU+wjgcdJsaeMQ/zsOK81fuuLTmkXvF0YfMRIVU6rMlci+Q/ZyyLFdt/n1U4V8wVK1YsWBRzJf+nUJ/8nAIYeWpccDoQmRZhgBKLo60dboSbR1Dw6hsa aaspbD364g4NX/Vyuqf+3PAcljw4MzlrKqsYmWLBIC7qy1ht7kQudOMhk+Lmj0BfyQ+/ROfgA+XsW93pCiW/+vZ/7g</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\SkypeLogo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 200 x 201, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4182
Entropy (8bit):	7.909192058088364
Encrypted:	false
SSDEEP:	96:GIGRHa4URXDu8y5PaMk8GBkm80f/tBy4BFMaAGETMmWIJSrr2Wz:GAgzy8yFk8iW0NBnHFAZTdbor/z
MD5:	989D94384251897332E40EE8D78E8699
SHA1:	103981B74664D6DC685DFBDBFF79A94E943B1433
SHA-256:	00D0FC4A8549E326DF3F9756507522FAA7C4CD4E2497E36776ABD952EF80720A
SHA-512:	8F461EFAE57075659AF1678AA31A6330FD903C699A47E9D2EAE8FA634C5AEE5B3E81BD743D537301A5B7C1ACC0D79E6A8C8C7985818371C172D3BFC2E20B181F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/SkypeLogo.png?version=094872a9-332f-ed1c-c1a7-356b86335212
Preview:	.PNG.....IHDR.....f.);.....pHYs..#.#.x.?v.....tEXtSoftware.Adobe ImageReadyq.e<....IDATx...u.J.....7...b*...S...0`*.. v.(.T.R.J...p5.....\..~.9{r.[.....c..?.4..wQ.#.6....9..+...ZB?.LF...Xs.....Q.]....Y.P.`.....0.v5.W.1,1.....C.....*.%... 6].9...~..f.%.....Zdm*....[...'q..N..g... 0>)..g...)..A..c.....0l.\$..8.a.T..<...b...@x. ..l(u.4X9.\$f`Rt...dp..j)\.....X...3n.baY!.....).V.....t.ol.R..m..)*...8...sPR.R/'8F.C^_...@i....(Y.kv....nU.8.z.....*.....p@%.gP./..>.TQ7..o...;PM...L.fce@x..'9.5...r..=5.....p@-E.g.n.....~..B.J..c.....l(.C.....J.C..b.(dQ...g.s....{+2,......}{ff,....."x.L.Z.=~.JA.\$.....%. ..HJ.....\$G.t.B..k./..2.l'.l..{[.~.(/f.r.....e...z.W.W3.....w...z4...mL.....s.hF...5.N.l.y.?#.....A...X...Mv.+y.@.z.l.r.-W.p.N:HNx.i-.....). 2.&2.....-.+}Kf.w....J.cM...j.e.....t.k.5..yJ..%.Y.....sQ.3u`.%...Z@.....X.2....hl..0N.l.J.;w

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\WindowsLogo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 94 x 94, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	14980
Entropy (8bit):	1.7787867610265293
Encrypted:	false
SSDEEP:	48:8YSN+k29W8sEvVxN+Y9QcmabBCgCxC5c4O+7uTSB8xYxtWpZjN:8FskEWRcxNXo5c49WNxYxEpL
MD5:	571BA43D6BDDDA3F287CA5B1EB2FD182
SHA1:	E6F18A86BD2CA5CCCF4651318DAA23D2808A388D
SHA-256:	868BF06E18AE90457FDC1B3FC1C31B394FAF81F4A168AD9C929EABB0992FD7DD
SHA-512:	0B8BDD48B0F53EFC7C824BF603D493A2B339FCED5D11E6907E3463CE60E3F1BA6F79951660F29ADC6427DED822BB0494BFF7F71FC247AA4041C8F8137F50E41D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/WindowsLogo.png?version=398e6d8c-a6fb-34d4-3af8-00da2a51e79a
Preview:	.PNG.....IHDR...^...^.....n.....pHYs.....g..R..8&iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?><x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmpptk="Adobe XMP Core 5.6-c111 79.158325, 2015/09/10-01:10:20 " >. <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#" x:mllns:tiff="http://ns.adobe.com/tiff/1.0/" xmlns:exif="http://ns.adobe.com/exif/1.0/">. <xmp:CreatorTool>Adobe Photoshop CC 2015 (Windows)</xmp:CreatorTool>. <xmp:CreateDate>2016-03-22T09:54:26-07:00</xmp:CreateDate>. <xmp:ModifyDate>2016-03-22T09:55:35-07:00</xmp:ModifyDate>. <xmp:M

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\azuremediaplayer.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	355277
Entropy (8bit):	5.393757002855038
Encrypted:	false
SSDEEP:	6144:9lBcZnQ9e9xUd1z40UOWpKfMpfhFIS5AcL04MGFu9g0ErFWlLeBC35hWNxX:LBq+eT6Vn
MD5:	ECF28ABBD888AEA2FDDE7D77CF64ABD5
SHA1:	BB285BFBC1FEC4915059172FAF07AD2F298DA13C
SHA-256:	5C02AA51C6CFEADA87DCE894669C060AD7F7A7DCD6C19E0D575040100B660D37
SHA-512:	3DDCFB502455FA6C06B4273C9AF089881C86B69FAB8530919BB3AB4D3BFEECDCCEDAE79019FAA373C68776BB305DF0B7E177CB64DC06C40B0381B47CA257EC
Malicious:	false
Reputation:	low
Preview:	/* Azure Media Player v1.8.0 (c) 2015 Microsoft Corporation */.function _handleMultipleEvents(n,t,i,r){vjs.arr.forEach(i,function(i){n(t,i,r)}))function _logType(n,t){var i,u,r; i=Array.prototype.slice.call(t);u=function(){};r=window.console[log?u.warn:u.error:u]?i.unshift(n.toUpperCase()+":"):n="log";vjs.log.history.push(i);i.unshift("VIDEOJ S.");r[r[n].apply?r[n].apply(r,i):r[r[n](i.join(" "))]]function Objecttron(n){var t;for(t=1;i=0,len=n.length;i<len;i+=1)n[i].isRoot?t.push("root"):t.push(n[i].name);var e=function(n,t){var i;if(n!=null&&t!=null)for(i in n)n.hasOwnProperty(i)&&(t.hasOwnProperty(i))?(t[i]=n[i]));u=function(n,t,i){var o,s,r,u,f;if(n!=null&&n.length!=0)for(o=0,s=n.length;o<s;o+=1)r=n[o],t.hasOwnProperty(r.name)&&(i.hasOwnProperty(r.name)?r.merge&&(u=t[r.name],f=i[r.name],typeof u=="object"&&typeof f=="object"?e(u,f):i[r.name]=r.mergeFunction!=null?r.mergeFunction(u,f):u+f):i[r.name]=[r.name]}},r=function(n,t){var f=n,o,c,s,l,h,i,e;if(f.children!=null&&f.child

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\E\0W10PBUV\cf-7c36ab[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):	168646
Entropy (8bit):	5.044051581582224
Encrypted:	false
SSDEEP:	3072:OzCPZkTP3bDLH0tfRqQ0xtLfj4ZDSlpTt813viY8R1j35Ap7LQZLPPJH7PAbOCxR:clZAXLkeedh
MD5:	0DCFF2779D4542C11AD9C9C19DF8328D
SHA1:	D7EFAE8E66FA6B4C335826BFD8C56C6F142E4254
SHA-256:	440D8292ABDF80DD6E8A9D9FAEA83367CE57BD1A1A8D153EDC358DB5F97EFF35
SHA-512:	CC747AA36ADEE4CBA4236F01820CE9661214C649DCF23227D7CF9187E24F2D15DBA43E9B706B30DC3D55060E08601575EAB0256306AEA28F3544BAD4BC33E913
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-eus-prod/west-european/shell/_scrfl/css/themes=default.device=uplevel_web_pc/93-de417f/39-6894a8/60-0f9daa/9c-879d19/5f-d422a2/ea-c61049/a7-5072ba/cf-7c36ab?ver=2.0
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\user1\AppData\Local\Microsoft\Windows\NetCache\E\0W10PBUV\le3-082b89[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):	114263
Entropy (8bit):	5.226391853242211
Encrypted:	false
SSDEEP:	1536:RL0mRvoBVfpuzUHQcyAz9ppxS7grUU59gQ9IwlnL2dS6J09RhY8WOyd1EwgXA9Gr:fzUnppxvleJ0y9d1EwgXA9JKinDCE54
MD5:	5C41C54A3D5E4E5D879F829A2AE7F469
SHA1:	B062A76379B0C8DD9FEF92342F4D2C536F6CAD2C
SHA-256:	3DC43C2A6F9E014EA7DC3A42CA3DFBE0BF0C5A28A42D493826734C7B13EFC915
SHA-512:	5A11FC7C315CBFE96CC827B5B505686408E08B013D3E05B1E583049C5B94127FAB27133E0B16A364D65DA9F676505CF0A109CC6104D01EFDEC4378FB0455E49
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/MICROSOFT-365/_scrfl/js/themes=default/c9-7b8600/2f-63ce8f/45-f9a0d4/aa-dc1460/2d-7a9063/dc-7e9864/4f-5115f8/7d-266f10/4a-abd94b/6d-c07ea1/29-1ec5a9/23-c64e70/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/b2-7087f0/e5-08f1c0/91-97a04f/1f-100dea/33-abe4df/50-f1e180/e3-082b89?ver=2.0
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\user1\AppData\Local\Microsoft\Windows\NetCache\E\0W10PBUV\icons[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), icons family
Category:	downloaded
Size (bytes):	4388
Entropy (8bit):	5.568378803379191
Encrypted:	false
SSDEEP:	96:2WZx42qACoApC6do8MPOGiN4mER38GTDfO/fv:1x42qAHAo6VMPi6mcTy
MD5:	77E1987DF3A0274C5A51E3C55CEE7C98
SHA1:	9B0FE96AF141AB09183F386F65BC627B8C396460
SHA-256:	EF04649D4D068673CF0FA47EF4C45C8BE291E703F4EC5FC0E507F17839120AA2
SHA-512:	B1E0CFB515FF2298799BA54574899D27B1FC043F66CC4E9591C504F88273B98697B99ED25955DB84986B39ED9F51864611833DC88064B14C29ADC020FBF6E295
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.onestore.ms/cdnfiles/external/oneui/oneui1.16.2/dist/fonts/icons/icons.eot?
Preview:	\$.....LP.....G.....i.c.o.n.s.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. 1...0.....i.c.o.n.s..... OS/2/@.Mn...(\..Vcmap.1.....Jglyf.....dhead. 9.....6hhea.\$.....\$hmtx@......loca". h...L...Bmaxp.3.`..... name.....post[NK.....G..._<.....T..... D.l...H.D.l.....PfEd.@.....D.....(.....

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\jquery-ui.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	238314
Entropy (8bit):	5.145714836445267
Encrypted:	false
SSDEEP:	3072:2xDkUPS1lippePIIYI7pSDzOyAskRsPoeQ9+SuC:yU+IgtYIUGeQ9XuC
MD5:	DfE3ECF96456F8CAFC12A7F48DE6B8C8
SHA1:	9927AFBB31DF93A76977A676A933B7E3696D61BA
SHA-256:	E09639315704980552B92EAAE21F66AF00A6E8A371F757F76B0B12420C2ED2A7
SHA-512:	3D892EE75916931C6E8743A24078BC20DC1F0C455C11EF49601899080DB51B421319D11453BB1C1214F2BADB7AF632B9F75BCA2660613CC3FEC9831DE89F3C9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ajax.aspnetcdn.com/ajax/jquery.ui/1.11.1/jquery-ui.min.js
Preview:	/*! jQuery UI - v1.11.1 - 2014-08-13.* http://jqueryui.com.* Includes: core.js, widget.js, mouse.js, position.js, accordion.js, autocomplete.js, button.js, datepicker.js, dialog.js, draggable.js, droppable.js, effect.js, effect-blind.js, effect-bounce.js, effect-clip.js, effect-drop.js, effect-explode.js, effect-fade.js, effect-fold.js, effect-highlight.js, effect-puf f.js, effect-pulsate.js, effect-scale.js, effect-shake.js, effect-size.js, effect-slide.js, effect-transfer.js, menu.js, progressbar.js, resizable.js, selectable.js, selectmenu.js, slider.js, sortable.js, spinner.js, tabs.js, tooltip.js.* Copyright 2014 jQuery Foundation and other contributors; Licensed MIT */.(function(e){"function"==typeof defin e&&define.amd?define(["jquery"],e):e(jQuery)})(function(e){function t(t,s){var n,a,o,r=t.nodeName.toLowerCase();return"area"===r?(n=t.parentNode,a=n.name,t.href &&a&&"map"===n.nodeName.toLowerCase())?o=e("img[usemap='"+a+"'"]")[0]!.o&&(o):1):(input select textarea button obje

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\latest[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Segoe UI family
Category:	downloaded
Size (bytes):	35047
Entropy (8bit):	7.975792390307888
Encrypted:	false
SSDEEP:	768:l6ibzTDpOGuAJ63YB9eSzDtQEspfAzyNyuBmOfAJYCM:/IPMYJ4GEAZoTyglcM
MD5:	CAD76E4816AF6890C9BFD02A6D1EA899
SHA1:	9EDC91541C31034FCE0D83AABBAAD4C314CD3D33
SHA-256:	D5794223D1A062E5DBE6C34C1994C8CE3792B24AFD5218D0644CB1F53DA4BE58
SHA-512:	24983A5856C2B4D8CBE2A4BD233A93B266A03D4218942E1D1733B33B65AB7A504AF0AC31DE2F1E69F6FF8CCD7A169CD455539D34FF8DE4CB8C98DB2DB2C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot?
Preview:	...=.....LP#...B.....S.e.g.o.e. .U.I.....R.e.g.u.i.a.r.....V.e.r.s.i.o.n. .5...3.2....S.e.g.o.e. .U.I.....RV.z.;~.....U.D.-.iu..N4Pl\GLFM .Y.?;...-~...Ox.M..".\$......g..s.c*2..4W....9AGc.[a.*.rCl]..@..U_..L...e..Ru.J.-.f..3.....S' .A.....K<;...n.Y...rfl.....([...W...5k.....^K.G...U @....2H..B.)N0w....C..9..... ..#..l2.4..6y.3\$b...K.wx...l.\$E..?3.8.c...x..t.wa.O...4.c...!+.<EM...2T>.\.j4.A.H.;.G.....W.:.?..Z".....e...8...84.L..)0..y.Xdd.Pa.@.&o(.l.q.yF...[.y.m(D...(....T.....A.;q.... .w\$.C..a. .Y.O?{..0...1.;C.....W..Q~.'.5tD@9..U..E4e.&_...S.Y..)\b.s.rfR.....R..KU O..{.0(.....^Q\^!et..Kf%.K...).1...S.{.....3p..].Y..w..JJeS\$.k.....>(8..ZIV..N.). c...Z.K..q.....'S.j.....9....._E.#s*#.....[.....DJ^L7./1...+U.qG.....-.MM..q...L..c..^....e....<h....`jz..fb.Ha....k.....e)g.l..".M

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\latest[2].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Segoe UI Light family
Category:	downloaded
Size (bytes):	28315
Entropy (8bit):	7.9724193003797
Encrypted:	false
SSDEEP:	384:+R0Z7+bHAtrQ1yBFbgqLct7JhhPLLkHsrvSzaJu4ml3n5o+MmKCxDg6IT7jdVye:+uNUAtE3phPLLFTiMu+pxCjHyGEQ9zL
MD5:	17DFE73CB9C64527F7248B0A24DB317D
SHA1:	345198B9239FCDAF038FB2D3A919E4724037DBAA
SHA-256:	AD75FB92B2EBCE6C37640F03E1AB96A752F388BCE60C877ADE4780B13839E8C4
SHA-512:	421B56D93E9BD5E4B4449DD0FCDEE8D531087FD484C91530AAF0A67EDEA33D5AC2F14A7F4966C528C0F130F17F26629FCAB9F8AB47E950CEB5B9F1A827EA0728
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.eot?
Preview:	.n...m.....LP#...B.....S.e.g.o.e. .U.I. .L.i.g.h.t.....R.e.g.u.i.a.r.....V.e.r.s.i.o.n. .5...3.2....S.e.g.o.e. .U.I. .L.i.g.h.t.....K.e.e.66.....U.D.-.iu...4Pl\GLFM.C?;...-~[...P..\.(.)RI.....>..CE..SsVjPR...H.....J.R.&.n.ht.....x.....qwA[...F.....c.".....Zed..>?...`.3...B..W...R...F.j...v..'?5.k^.....+.a...). _]x.#QSi... <t...k...Hv1.G...L\$.9...5.t...V.Y..... . @...B.....P`..2.Z.O...2'.FR.MF8.x...GP0.\$...PYm.22..."S".1.*j[.=.mR.*.....j....&4..k..}1@..y\$....."y..C..g7..kB*. _V..F...G.m.jK ...O...b.Qlo...!N.V...t.t[.p.N...~@1d...YX.."...R_i.4.\$j.P.U...u9...<.6.4%.....9'.....S...N.Y..L.B\$2\E.vhe...n..h.5.Z.K?H..S...2.=R.x....EX.2.....\$. ".... lI8..z.+h ..\$.2*T...jZ../...p..b0ae.qq.(v1..E.l!"a.p.);..8t..7..^..W...4A.DleOb\$.....b.Nl.Pe.#\$.O38.....g.&[...B{...}....9..u.8..~Y...3.X..ff.,

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\me[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	10320
Entropy (8bit):	5.440510239263796
Encrypted:	false
SSDEEP:	192:BDC1n+7Xr+cHEzFQD6Ds35b05e58ITZSTXh7gk0yi4BWMmt88:BT7XrUJds35bd8cAA1
MD5:	AD3A1CD10D65EFB55C9DF77DF9B60BE0
SHA1:	369FFAA989766EFA01B438F2EF3CF5FB35EBAC0
SHA-256:	5FFC8E186F57C83D7DDCBDA7A1C52B31520A7CE3FF82C21AA1BA22F6D511DC2F
SHA-512:	7A19C301850006485FEE07EDD2F26B1C0B8495236529FA9B552427D9BCC5CD9DCC77A6E8C2F75BC8710893F1E0D343AE393465F30471D1FDFE536C1B7AB4D8C
Malicious:	false
Reputation:	low
Preview:	Copyright (C) Microsoft Corporation. All rights reserved. --><!DOCTYPE html> ServerInfo: BY1PPF521859390 2021.01.08.00.05.12 Live1 Unknown LocVer:0 --> P reprocessInfo: azbldrun:AzBuildCU-Ha02, 2021-01-07T23:53:46.6990514-08:00 - Version: 16,0,28893,3 --> RequestLCID: 1033, Market:EN-US, PrefCountry: US, LangLCID: 1033, LangISO: EN --><html dir="ltr" lang="EN-US"><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"/><base href="https://lo gin.live.com/pp1600/"><noscript><meta http-equiv="Refresh" content="0"; URL=https://login.live.com/jsDisabled.srf?mkt=EN-US&lc=1033&uid=5ffa7d6c561a4 bd2c4b493c1a8d09225"/>Microsoft account requires JavaScript to sign in. This web browser either does not support JavaScript, or scripts are being blocked.
<br </To find out whether your browser supports JavaScript, or to allow scripts, see the browser's online help.</noscript><title>Windows Live ID</title><meta name="robots" content="none" /><meta name="PageID" con

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\meversion[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	27565
Entropy (8bit):	5.240358934595407
Encrypted:	false
SSDEEP:	768:p0Y26BzK4ey2FvZ60dQCn16JD2BIRnusqer6tAH6teJuN:72AzK4ey2FvZrRdQ3JD2BXAY6tAH6teJc
MD5:	B9AC7ED55AA986167869B6A1D2B908FD
SHA1:	469D737A86B343632FAD5EEF2EB40DA10FE6F3F8
SHA-256:	99121416EE3007784D14585CEFB1A32130E132150D8E9828D6B88B0535C1D03B
SHA-512:	2A180E97F3833F3054354FCA5A217B0B034342D143312C456476169665107E5D0C5BF63A31074D0A6D212C46D6E9E6E548304B504ADF652FEED649A5E343486
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://mem.gfx.ms/meversion?partner=OfficeProducts&market=de-ch&uhf=1
Preview:	window.MSA=window.MSA {};window.MSA.MeControl=window.MSA.MeControl {};window.MSA.MeControl.Config={"ver":"10.20321.2","mkt":"de-DE","ptn":"officepro ducts","gfx":"https://mem.gfx.ms","dbg":false,"aad":true,"int":false,"pxy":false,"msTxt":false,"rwd":true,"telEvs":"PageAction, PageView, ContentUpdate, OutgoingRequest, ClientError, PartnerApiCall, TrackedScenario","remAcc":true,"main":"meBoot","wrapperId":"uhf","cdnRegex":"^(?:https?:\\V\\V)?(mem\\.gfx\\.ms(?:\\.)?)controls\\.account.mic rosoft(?:[-int]-dev)?(\\.com)?(?:[0-9]{1,6}) amcdn\\.ms(?:ft)?auth\\.net(?:\\.)?","timeoutMs":30000,"graph":false,"aadUrl":"https://myaccount.microsoft.com","msaUrl":"http s://account.microsoft.com/";window.MeControl=window.MeControl {};window.MeControl.Config={"ver":"10.20321.2","mkt":"de-DE","ptn":"officeproducts","gfx":"https ://mem.gfx.ms","dbg":false,"aad":true,"int":false,"pxy":false,"msTxt":false,"rwd":true,"telEvs":"PageAction, PageView, ContentUpdate, OutgoingRequest, ClientError, Partne rApiCall,

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\meversion[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	27551
Entropy (8bit):	5.240675050935438
Encrypted:	false
SSDEEP:	768:L8Y26BzK4ey2FvZ60dQCn16JD2BIRnusqer6tAH6teJuN:12AzK4ey2FvZrRdQ3JD2BXAY6tAH6teJc
MD5:	38DC0F2AD21EC30A915E48510428E7DB
SHA1:	B30BC7B718DBC28DFAF38A6FC0E377D07B6FDD4B
SHA-256:	EBC5A77E1D7C196EAEDF46F1ACD7748282D136DC47530EA00FFDC8AD28882C75
SHA-512:	92DE24E05E089FA740E7F48F0A128998C6E36F0D0E42C46121513B4553FA6F7C58952D7B2084642FE6ACFF36121532C2BE127F150C3CAC0972DCD4E63233C3C5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://mem.gfx.ms/meversion?partner=windows&market=en-us&uhf=1
Preview:	window.MSA=window.MSA {};window.MSA.MeControl=window.MSA.MeControl {};window.MSA.MeControl.Config={"ver":"10.20321.2","mkt":"en-US","ptn":"windows", "gfx":"https://mem.gfx.ms","dbg":false,"aad":true,"int":false,"pxy":false,"msTxt":false,"rwd":true,"telEvs":"PageAction, PageView, ContentUpdate, OutgoingRequest, ClientE r, PartnerApiCall, TrackedScenario","remAcc":true,"main":"meBoot","wrapperId":"uhf","cdnRegex":"^(?:https?:\\V\\V)?(mem\\.gfx\\.ms(?:\\.)?)controls\\.account.microsoft(?:[- int]-dev)?(\\.com)?(?:[0-9]{1,6}) amcdn\\.ms(?:ft)?auth\\.net(?:\\.)?","timeoutMs":30000,"graph":false,"aadUrl":"https://myaccount.microsoft.com","msaUrl":"https://acc ount.microsoft.com/";window.MeControl=window.MeControl {};window.MeControl.Config={"ver":"10.20321.2","mkt":"en-US","ptn":"windows","gfx":"https://mem.gfx.ms" ,"dbg":false,"aad":true,"int":false,"pxy":false,"msTxt":false,"rwd":true,"telEvs":"PageAction, PageView, ContentUpdate, OutgoingRequest, ClientError, PartnerApiCall, Trac kedScenari

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\microsoft-office[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	207181
Entropy (8bit):	5.292022836302801
Encrypted:	false
SSDEEP:	1536:0HmlR3dyJ9Zm4nzKF5ZHgKh1LGYhz3jEj9TNfHx7EmI9o/W+7YupJypWqxWCTj6Q:0lR3dALU4Y0W+7YupJypNtWfY
MD5:	01EB09021D97D034122EB916F5808207
SHA1:	C065CD6827A8AB5CE6B81B297231D676D4932539
SHA-256:	18DC63F6AA49DC04D9323EFFBFEE1F7C66954423F6FF043C14EDB4A6AE39BDD6
SHA-512:	1B937247A8683DEE1E67D1AE90673DDDA227E0C63933AC86C2F2C0B31A042241E6E49F92253D5C5C064B86FD4647E35D1C18B926FFE50848D5B7F9367E5C9D5
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>...<html lang="en-us" dir="ltr">...<head data-info="{"v":"1.0.7662.39393","a":"5b7ee488-9b1e-4c6f-a5af-1a893be84d2","cn":"OneDeployContainer","az":"{did:92e7dc58ca2143cfb2c818b047cc5cd1, rid: OneDeployContainer, sn: marketingsites-prod-odnortheurope, dt: 2018-05-03T20:14:23.4188992Z, bt: 2020-12-24T05:53:06.000000Z}","ddpi":"1","dpio":"uot,","dpi":"1","dg":"uplevel.web.pc.ie","th":"default","m":"en-us","l":"en-us","mu":"en-us","rp":"en-us/microsoft-365/microsoft-office","f":null,"bh":;}}">...<meta charset="UTF-8" />....<meta http-equiv="x-ua-compatible" content="ie=edge" />...<meta name="viewport" content="width=device-width, initial-scale=1" />...<title>Microsoft Office is pa

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\mscom-grid-mixed[1].css	
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):	143317
Entropy (8bit):	5.038817397019549
Encrypted:	false
SSDEEP:	3072:rz3i3xD5xBXZHMWqyolV2qy0lXK14C3bvcx/zuJ0VVgJl0wqHZq3J2ffrCfbkpC:XyolV2qy0lXK14C3bvcx/zuJ0VVgJl0a
MD5:	8A8DDDFEC472B08925BE8BA81616CD917
SHA1:	26BECF031E1C86F3812B16C295768B0BCB0E95EB
SHA-256:	2743B78020B1AE45E5D8FB8CF68671813D4B5CA021B3FE977AA631D6445C7E9A
SHA-512:	AE7F9D7D98DFA367EB0F370B3DFB4CEC7AE11A625D444FBCE98D09D4C4F48691EB263F983B28A0B9C5A97852CB9853F34078F3D18B31F5307E30E36493E8A33D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.xbox.com/en-us/global-resources/Picchu-Grid/CSS/mscom-grid-mixed.css
Preview:	.ms-grid,[class*=col-]{width:100%;position:relative}a,abbr,acronym,address,applet,article,aside,audio,b,big,blockquote,body,canvas,caption,center,cite,code,dd,del,details,dfn,div,dl,dt,em,embed,fieldset,figcaption,figure,footer,form,h1,h2,h3,h4,h5,h6,header,hgroup,html,i,iframe,img,ins,kbd,label,legend,li,mark,menu,nav,object,ol,output,p,pre,q,ruby,s,samp,section,small,span,strike,strong,sub,summary,table,tbody,td,tfoot,th,thead,time,tr,tt,u,ul,var,video{margin:0;padding:0;border:0;font-size:100%;vertical-align:baseline}.ms-grid,.ms-row,[class*=col-]{box-sizing:border-box}.ms-grid{display:block;margin-left:auto;margin-right:auto;max-width:1600px;padding-left:12px;padding-right:12px}.ms-grid.fixed .ms-row,.ms-grid.fixed-small .ms-row{margin-left:-2px;margin-right:-2px}.ms-grid.full{max-width:none;padding-left:0;padding-right:0;width:100%;overflow-x:hidden}.ms-grid.fixed .ms-row>[class*=col-],.ms-grid.fixed-small .ms-row>[class*=col-]{padding-left:2px;padding-right:2px}.ms-grid.fixed-lar

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\mwf-auto-init-main.var.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	307257
Entropy (8bit):	5.169381678188456
Encrypted:	false
SSDEEP:	3072:09GZepVIQHj9bOFGBiXZcwW9L4szVbkps2M3gV4L:09GNW9BBKw9oiFL
MD5:	BFCD48223E39F7A846413DD5814365E9
SHA1:	13DDB26618D203607C9B12D0D0D80F03ECB71362
SHA-256:	5E484A06AE85C5A599A6511224405A773FB3AF3D9D6600AF8F5A1B4A2C39504F
SHA-512:	FD66AA707E23432C48C5709CD75C2235850884F198B339EEA8238395A0B875ED7890AA2A04DFDF82E46C152CA7ECE88EA2B4C64C978C94BF84E274BF47A049E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.onestore.ms/cdnfiles/external/mwf/long/v1/v1.22.1/scripts/mwf-auto-init-main.var.min.js
Preview:	#!/ modernizr 3.3.1 (Custom Build) MIT *. * https://modernizr.com/download/?-eventlistener-picture-printshiv-setclasses !*/.!function(e,t,n){function r(e,t){return typeof e==t}function a(){var e,t,n,a,o,c,l;for(var u in s)if(s.hasOwnProperty(u)){if(e=[],t=s[u],t.name&&(e.push(t.name.toLowerCase()),t.options&&t.options.aliases&&t.option s.aliases.length))for(n=0;n<t.options.aliases.length;n++)e.push(t.options.aliases[n].toLowerCase());for(a=r(t.fn,"function")?t.fn():t.fn,o=0;o<e.length;o++)c=e[o],l=c.split it(" "),1==l.length?Modernizr[l[0]]=a:(!Modernizr[l[0]] Modernizr[l[0]]instanceof Boolean (Modernizr[l[0]]=new Boolean(Modernizr[l[0]])),Modernizr[l[0]][l[1]]=a).i.pus h((a?"":"no-")+l.join("-"))}}function o(e){var t=l.className,n=Modernizr._config.classPrefix "";if(u&&(t=t.baseVal),Modernizr._config.enableJSClass){var r=new RegExp("(^ \\s)"+n+"no-js(\\s \$)");t=t.replace(r,"\$1"+n+"js\$2")}Modernizr._config.enableClasses&&(t+=" "+n+e.join(" "+n),u?t.className.baseVal=t:l.className=t)}

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\mwf-auto-init-main.var.min[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	298040
Entropy (8bit):	5.170582206405612
Encrypted:	false
SSDEEP:	3072:09GZg9tIQHj9b1skD1nPwwwW9/xNS/xg4DJ3P26:09GrW9/DCW9Yhu6
MD5:	9CA3E3920A1FB6F3A5D3FA1F40DA56F0
SHA1:	F4AC5E5BA4422919F4CC9A8499D672754F840CE4
SHA-256:	A5E5538AB72F6C15A94665A0828BECCE00BD96113DD7CBF877FB169CCE809AA
SHA-512:	D1979F0C625F9293D4E27608AC74566F71EF41995FF76E021C037726D93A45488F7A0F8F4353ADA9E39C058B77C65294BCAF7245B2EA20914E700AA773290649
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.onestore.ms/cdnfiles/external/mwf/long/v1/v1.23.1/scripts/mwf-auto-init-main.var.min.js
Preview:	<pre>#!/ modernizr 3.3.1 (Custom Build) MIT *. * https://modernizr.com/download/?-eventlistener-picture-printshiv-setclasses !*/.!function(e,t,n){function r(e,t,n){return typeof e===t}function a(){var e,t,n,a,o,c,i;for(var u in s)if(s.hasOwnProperty(u)){if(e=[],t=s[u],t.name&&(e.push(t.name.toLowerCase()),t.options&&t.options.aliases&&t.option s.aliases.length)}for(n=0;n<t.options.aliases.length;n++)e.push(t.options.aliases[n].toLowerCase());for(a=r(t.fn,"function")?t.fn():t.fn,o=0;o<e.length;o++)c=e[o],l=c.split(""),1===l.length?Modernizr[l[0]]=a:(!Modernizr[l[0]] Modernizr[l[0]]instanceof Boolean (Modernizr[l[0]]=new Boolean(Modernizr[l[0]])),Modernizr[l[0]][l[1]]=a),i.push((a?"":"no-")+l.join("-"))}}function o(e){var t=l.className,n=Modernizr._config.classPrefix "";if(u&&(t=L.baseVal),Modernizr._config.enableJSClass){var r=new RegExp("(^ \\s)"+n+"no-js(\\s \$)");t=t.replace(r,"\$1"+n+"js\$2")}Modernizr._config.enableClasses&&(t+=" "+n+e.join(" "+n),u?l.className.baseVal=t:l.className=t)}</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\mwf-main.var[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	975923
Entropy (8bit):	4.534114714730074
Encrypted:	false
SSDEEP:	12288:Mf6A3YtFg2jgDgUQZ+MLFPXTrK7Zy8viqtX5lXj5PsG4UJf0l/tcpKR3+MMrOfF:MSVl/BvVclQPH
MD5:	0757357BA2567A518EAF8EB0723677E1
SHA1:	CC3EB31A04544F1A7257A0810FA09576E56035CB
SHA-256:	ED8A2123175AE5DBC6A22DA8B479DACDA8F255FC21274A40ABFA7E7B6EB5676
SHA-512:	2168E1938C3E8A9FB006DF32805EACB541CD947DE7C97338D574E51440591D3D75537AFCB8BEC02CE32E51B719A4853C41C2770C0C5FF259CC668C87E60B106
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.onestore.ms/cdnfiles/external/mwf/long/v1/v1.19.1/scripts/mwf-main.var.js
Preview:	<pre>var mwf = /*****/ (function(modules) { // webpackBootstrap./*****/ .// The module cache./*****/ .var installedModules = {};./*****/./*****/ .// The require function./*****/ .function __webpack_require__(moduleId) {./*****/./*****/ .// Check if module is in cache./*****/ .if(installedModules[moduleId])./*****/ .return installedModules[moduleId].exports;./*****/./*****/ .// Create a new module (and put it into the cache)./*****/ .var module = installedModules[moduleId] = {./*****/ .exports: {},./*****/ .id: moduleId,./*****/ .loaded: false,./*****/ .};./*****/./*****/ .// Execute the module function./*****/ .modules[moduleId].call(module.exports, module, module.exports, __webpack_require__);./*****/./*****/ .// Flag the module as loaded./*****/ .module.loaded = true;./*****/./*****/ .// Return the exports of the module./*****/ .return module.exports;./*****/ .};./*****/./*****/./*****/./*****/ .// expose the modules object (__webpack_modules__)./**</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\override[1].css	
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):	1531
Entropy (8bit):	4.797455242405607
Encrypted:	false
SSDEEP:	24:UdfoF+MOu2UOqD3426TKgR2Yyk9696TkMYqdfskeEkeGk/ksuF9qaSm9qags:Ud8FYqTj36TKgR2Yyk9696TkMYO0keEW
MD5:	A570448F8E33150F5737B9A57B6D889A
SHA1:	860949A95B7598B394AA255FE06F530C3DA24E4E
SHA-256:	0BD288D5397A69EAD391875B422BF2CDBCC4F795D64AA2F780AFF45768D78248
SHA-512:	217F971A8012DE8FE170B4A20821A52FA198447FA582B82CF221F4D73E902C7E3AA1022CB0B209B6679C2EAE0F10469A149F510A6C2132C987F46214B1E2BBBC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://statics-marketingites-eus-ms-com.akamaized.net/statics/override.css?c=7
Preview:	<pre>a.c-call-to-action:hover, button.c-call-to-action:hover{box-shadow:none!important}a.c-call-to-action:hover span, button.c-call-to-action:hover span{left:0!important}...c-call-to-action:not(.glyph-play):after { right: 0!important;} a.c-call-to-action:focus,button.c-call-to-action:focus{box-shadow:none!important}a.c-call-to-action:focus span,button.c-call-to-action:focus span{left:0!important;box-shadow:none!important}...theme-dark .c-me.msame_Header_name {color: #f2f2f2;}...pmg-page-wrapper .uhf div, .pmg-page-wrapper .uhf button, .pmg-page-wrapper .uhf a, .pmg-page-wrapper .uhf span, .pmg-page-wrapper .uhf p, .pmg-page-wrapper .uhf input {font-family: Segoe UI, Segoe UI, Helvetica Neue, Helvetica, Arial,sans-serif !important;}...@media (min-width: 540px) {.pmg-page-wrapper .uhf .c-uhfh-alert span, .pmg-page-wrapper .uhf #uhf-g-nav span, .pmg-page-wrapper .uhf .c-uhfh-actions span, .pmg-page-wrapper .uhf li, .pmg-page-wrapper .uhf button, .pmg-page-wrapper .uhf a, .pmg-page-wrapper .uhf #meC</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\privacy-report[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	75051
Entropy (8bit):	5.208394364586097
Encrypted:	false
SSDEEP:	768:vOEaTN6uayKTKfSSkQgGscLkEuFEoW1G9ottlIiGicPRuDdueyaaFpdaHqGQKeJ:vOEM6HyrsmjNJ
MD5:	C1ED9857927008135E2AAB3B51B03F72
SHA1:	32DB1775AAD2AD8505E3565032DE8DFB7ED4833A
SHA-256:	9A4B0AF0FFB3219964E756316B1F396B8DD446CEF1C4B2E7A7290F2AC63F9FCE
SHA-512:	2037FE17EAE1B9C5AF50DF22BB44AD7AF7E93E5A8A0BCEE6590653EAB7402F481090F2CBD1347EDF11514B90881C5EA43E64BAB0B8C7A6E8AA50A83931C55ED7
Malicious:	false
Reputation:	low
Preview:	.<!DOCTYPE html ><html xmlns:mscom="http://schemas.microsoft.com/CMSvNext" xmlns:md="http://schemas.microsoft.com/mscom-data" lang="en-us" xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta charset="utf-8" /><meta name="viewport" content="width=device-width, initial-scale=1.0" /><link rel="shortcut icon" href="//www.microsoft.com/favicon.ico?v2" /><script type="text/javascript" src="https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js">.. // Third party scripts and code linked to or referenced from this website are licensed to you by the parties that own such code, not by Microsoft. See ASP.NET Ajax CDN Terms of Use - http://www.asp.net/ajaxlibrary/CDN.ashx... </script><script type="text/javascript" language="javascript">/*! [CDATA[*(function(d){if(d document).bind("mobileinit",function(){\$.mobile.autoinitalizePage=!1}),navigator.userAgent.match(/(Mobile 10\.[0])/){var msViewportStyle=document.createElement("style");msViewpor

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\script[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):	378046
Entropy (8bit):	5.33285538850032
Encrypted:	false
SSDEEP:	6144:DkQre4Pi4Sj1KhznflhL57EE6qQdoPn13lndKY9nY6lrWYC3GUYaY0YzYLOYd/t:W4Pi4Sj1KhznNhL5AjqOdCIS8sYv8
MD5:	532A1EC5DF65B8A5294CD3E4F1BCD30D
SHA1:	4BB498CEAC1FA6F244EC85F16D015E8D4D8E839A
SHA-256:	9CD4CBB1A567356BDB956F73C64B04289459AD780F12F1554D59D934D0ECF0A5
SHA-512:	0A799F3A8584240B7FD01F24077CFF3A1B5B1FDC0533C105254B30331EA60A79F19528981F9E412E51B89C10A4B8313FA46E4E9AAE3756DAB3FD7054EB47281D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=a99b0db8-bfbf-545e-1fb8-9506657ef0a2_548ab34c-2019-5a40-159d-497aca0a31aa_681f815f-66fa-dd0d-337c-f122e5fbc441_03f654df-21f3-ee95-3e73-ffff757267bc7_8b6e2c63-6927-7db5-8e32-7f3333da659e_336509cc-abc8-912e-9a27-74fc22d5e823_d05d04f0-2693-ec0c-01de-808f5ad22891_693cb7af-5841-0401-bf99-98f0d9ba4140_a42d7277-10a1-6935-b06a-ebeeb8815ba6_30431ce6-63a7-f889-dfb0-0df5e1561da0_a96731a9-c05d-ced4-6287-89c900b1ed4f_55f6f45b-01ff-8a72-87f2-aeef7adb3c4ae_2d3684a3-f1a0-d1c4-8c01-8f5b22b0884d_bec3e8b8-6afd-a4da-0cb7-e3f0e65d6704_25785618-c6df-5018-c882-7493400f3937_3df6f4407-99a7-efc0-9273-2886b50fa823_544bfecd-07c5-9fff-20c9-9125b66a3749_cc850638-66c6-0dc0-e5df-a231bf28e478_b1b02b3b-d9e7-9af4-8de2-ac45166d7cd4_88257d23-e3fb-0deb-d967-418273373312_79c01e4e-6436-0168-278f-66f180dd4fdd_360dd1e2-0971-6b97-6b15-bebe0e7ed91e_548c8edb-b925-5700-12de-1fbe1e801b5e_e102ee4d-7772-ae41-a83e-3b7ad65995ca_d707f600-5853-342b-4975-ecd516bff797
Preview:	#!/ picturefill - v3.0.2 - 2016-02-12. * https://scottjehl.github.io/picturefill/. * Copyright (c) 2016 https://github.com/scottjehl/picturefill/blob/master/Authors.txt; Licensed MIT. */.#!/ Gecko-Picture - v1.0. * https://github.com/scottjehl/picturefill/tree/3.0/src/plugins/gecko-picture. * Firefox's early picture implementation (prior to FF41) is static and does. * not react to viewport changes. This tiny module fixes this.. */.function RunPicturefill(){for(var t=jQuery("picture"),n=0;n<t.length;n++){jQuery(t[n]).children("img").each(function(){var u=jQuery(this).attr("data-src"),r=jQuery(this).attr("media"),f=function(l,r){jQuery("source",{media:i,srcset:r}).appendTo(t[n]);switch(r){case"(min-width:1779px)":case"(min-width:1400px)":case"(min-width:1084px)":case"(min-width:768px)":case"(min-width:540px)":case"(min-width:0px)":f(r.toString(),u);jQuery(t).remove();break;default:var e=jQuery(this).attr("src"),o=jQuery(this).attr("alt"),s=jQuery(this).attr("class"),i=jQuery(this).

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\skiptomain[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	112081
Entropy (8bit):	5.163346187487952
Encrypted:	false
SSDEEP:	1536:GV8Utc49kADAKlyvpkiLOOQeI4PQ4LqByzOafWLznLXAiQhnlOc8Sii7nm/zngp:slyvpkiLgCLSz71/z0
MD5:	6ECB014D8A69CDFBFE574EC593162A8F
SHA1:	7F61777B8A169B3964F6E4FBDDC59BFF8337EFE
SHA-256:	8A8E012BF50450A1A5D5DFA187CA4F1AEE0FBFC89967F6EF50F614B819D29BB1
SHA-512:	3B0B513ECE46E45115D30F5B3EBB3F403AFC2B5A6897ACCEC3BAC474C25D41E12EDA9EDA39E475BD4AF317BA79FE0987DB6BAC38ACA260638585659D33DCf6D6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/mwf/js/MWF_20200416_22921869/alert/areaheading/autosuggest/channelplacement/channelplacementitem/contentplacement/contentplacementitem/contentrichblock/flipper/flyout/glyph/heading/highlightfeature/hyperlinkgroup/image/list/pagebehaviors/singleslidecarousel/skiptomain?apiVersion=1.0

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\skiptomain[1].js	
Preview:	<pre>define("componentFactory",["require","exports","htmlExtensions","utility","stringExtensions","pageBehaviors"],function(n,t,i,r,u,f){"use strict";Object.defineProperty(t,"__esModule",{value:!0});var e=function(){function n(){}return n.create=function(t){for(var i,r=0,u=t;r<u.length;r++){if(i=u[r],li.c&&li.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 li.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=[c,o?(o.mwflInstances (o.mwflInstances={})).o.mwflInstances[n]?u.push(o.mwflInstances[n]):(h=new t(o,e),(h.isObserving h.isObserving())&&(o.mwflInstances[n]=h,u.push(h))))):cons</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\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:wIDY+ngX4zrTb52TyqydrTDZnaygTjwpykpw4blytWOUcqP2:wJRnhsyqsjZnayEkp7bUtWOUcqP2
MD5:	60B33E181A383283E6E96A9F40BF4045
SHA1:	7BF1BE1FE9AE44A1F94BFF9DA0C53D75715328C6
SHA-256:	AD6C804544415CFE232BC74D83F39989F4D2D4EB187A6ACB07FD6ECDE2493A33
SHA-512:	11EAA578B152228D4C2611106F8D34CD59556C0614DDED6418EFC8714AC39C88A7EDDDA61DC751ADF5FA979F4D30B8353540992960249AA9E927F8E94452C0C
Malicious:	false
Reputation:	low
IE Cache URL:	http://c.s-microsoft.com/en-us/CMSImages/1083_Panel15_Mosaic_Item1_Gray.jpg?version=38f7b9fc-53ec-4997-cd72-7fedd363404d
Preview:	<pre>.....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.....</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\1083_Panel15_Mosaic_Item2_Nocamera[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 542x400, frames 3
Category:	downloaded
Size (bytes):	30919
Entropy (8bit):	7.954402391877308
Encrypted:	false
SSDEEP:	768:gsgdbRBQEbYYA2dywOyLLNvR38w+VSbm2pRwfn8awr2:g9FvQEbyYYAveLLJsLSAn8aj
MD5:	EA6D26EF76C43E0E8765BF883564ACBB
SHA1:	7282DCB1FA4E9A45E3D92A9DD4BFA402B0D0E531
SHA-256:	679CF0C789EA0674002B3BAC1EDE7520E0A756B33187456F50207D4F44B43B09
SHA-512:	D45B31964251B2BFCD740D24E3A3B3202128248AD48CA0F0435315A73FBC155932398176D2E460E64008C77060FF7A4309943401E52CA3B35DFDBDB657BBCD0C
Malicious:	false
Reputation:	low
IE Cache URL:	http://c.s-microsoft.com/en-us/CMSImages/1083_Panel15_Mosaic_Item2_Nocamera.jpg?version=54716647-eadb-d215-11b6-adfd27375b54
Preview:	<pre>.....JFIF.....j.u...+.w].d...H.je..._.....u =.\$J.@.1.....P.....q5.G.....?a/..R.)AUm.H.'.....S...W.....C'.Uu..jV.....0.....Z...M/O.:j.....JD.b.....+.....l.....\..yN.....J'.d.:S.....F..\$...[.U.y..u.....B(HH...u.^.....\$ e..Qg.....&..z..ru.c.H.....OO.....4.^#W.iZ..W.IW..JHB...U.g..l...<.V.0@.\$..%:'n'..W..'l...!6.l.....j]tL.....u>...<A.C.l.m.....KH&x...n.f.>9.)m2.o%oA.~o.z.....u.cL..J..d.. j=.z.k...M...`S...f.[\...M...UuY*..T..Q.ol.j....Km..%\$J.....z..}.H."U.):t...Z...x<.F...T..D.z'...5..l..r.Y.o...R...t.M'E65.M.t...3..j[Gvw.i%111."q..{.u...9...l...S.S.{...X....l.(T..y. #..}.....c..<.....[...s.(IM... ..y..~.....[.#71.@.q.+>b..u.v... ,qAm.t....<u.....@.O.9...m.F..1.</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\1083_Panel15_Mosaic_Item3_Pen[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 542x400, frames 3
Category:	downloaded
Size (bytes):	38323
Entropy (8bit):	7.946783423203652
Encrypted:	false
SSDEEP:	768:8+YJ7M4lBm0zAWxb7asSZbuEdNZ10YgSnhYP0DXLADzLnZRAAl+dIVF:a1Mp6+ZZbusZ1WP0DXL+zLnZrAkQID
MD5:	A830AF5B34DC045823336439F57A5BDB
SHA1:	FD33215E86D0B2ED32CE565AA1C3DF109B243A93
SHA-256:	88DC7852D0D04B0B50C75776D3467028637D47C6D1D3E1961CE5A2AB56FEC0D5
SHA-512:	BE671F53EA853BE3B11CCAFCE276371928879E97110C4CAB786442CA19D6BAEB528BBC7ED619B9F59B3A0D5392B555EFEBEA5BB22E942E388362BC6A5FD515611
Malicious:	false
Reputation:	low
IE Cache URL:	http://c.s-microsoft.com/en-us/CMSImages/1083_Panel15_Mosaic_Item3_Pen.jpg?version=9f1f76fd-32d3-1aa3-4eec-e1fdab956923

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\1083_Panel15_Mosaic_Item3_Pen[1].jpg	
Preview:	JFIF...../kcklL1~7.m.+m...6-g7f... ..u.1..H...~....._Z.....P.....?.....%f3.gK\w...R.d.u.n.8..Y5...v.4....*..s-.....>...\$P:..t.kr.=?F/W.'.....=H...e..Dly.q.....e..Fb.....&..(p_...G?q:.....].%p.B...."....]#r.. ..5;v6.."]..]w...9f.....BaB..v.-F..Q...k.....O.Q.U.....e)IE.H.a-...=..={.7^...8{.Cm.\O.....9Dn.....g.....^S6*.6.p%?..Y.W1....k.....Ht....#...6...v...b..W_...^...c.2..O-<..... ...C(.....8.T.Wv..bjj....(.....n.=a..A.y{..2...V..+H.^s_ BX.<.....V.Y.[...j..L.7o.A\X....k..W:([...z/-...n.e.....A[.^.f...q.....c.c;.....\.....S3...WGc;...og;...Ga.S.]-.YQ.. ".....KSnM...O..E.&Z.gr.c.cq~...O.....u.1.#\5.5..K.tr5]..G.3W.....*C..r..tm. n-...lw\.....c..

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\1083_Panel15_Mosaic_Item4_Key[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 542x400, frames 3
Category:	downloaded
Size (bytes):	32390
Entropy (8bit):	7.962376262587795
Encrypted:	false
SSDEEP:	768:BlvLs1yU28KxNBdFs/g4ZYZVrmwKiZOe+d1/:yeyUhK77FsooYrtK3e8/
MD5:	6B4059FADC0A315A85CC23C9C4E22C35
SHA1:	373B35359E265D70F277C73BB51ED2A11F6AF74F
SHA-256:	676B72418905F920FA07A00D4AE96539396C52D61137A7B3BD506429CA79CC5A
SHA-512:	44D42215B506476822F3B653E3084C87743C116D211586DCA18AEB3FD93ECA4ACDEDB210E73DD649B6209AF8EF67CF0C4A2CA193B89D66D200D517A0FD3319
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1083_Panel15_Mosaic_Item4_Key.jpg?version=271e8d93-8c40-1812-9247-ef1a3ecd6392
Preview:	JFIF.....G.{....M.....5....^...NF+....DV.G bU..r.m.=/w.hC.i.....%m...N.....\$O.u..N....or.w.z.Q#..2..UUJv.....(.3;....*A""""F...9]...O..6...U%'.0.y.%`...Y.F...kb.G.....E.bj].. ".....mk%O...H.T....2.-...q..@A.PPS..i.m]... (A.`"""-i.=L.H.V.=.l.....eq`.T.@...l.J.\$..0.%x....222".....l.YX.G.@...g.0^x([...6.Y..URRi%V.....-sQ.\.i.....x.x..F..J.UH..X...E8.3p....3.Z...Dps.M5..`=.....H....)..lp.q..6:K.1ly{....G...`.m.m.6.]...d...l.c...V.OEx.....oK.%U..G....s.1Nj..m.i...jo1...W..Kj.Rf..b.3Ey.....<.../Y..A.l<...L=...i.k...22..w.XJ..o.l!n8..l.Xh.2.....\..J:]...J.V...."ed...Ji..xP.. .lA..k...q..r.u..2...{.....N#OIO.&k.1>3..t...h..Fijn..F3#p.q..q-...n.cz].?.m.(<.c.'M...;q..=#....c.Sckf...q.*.n...<...m

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\1083_Panel15_Mosaic_Item5_Stand[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 542x400, frames 3
Category:	downloaded
Size (bytes):	16475
Entropy (8bit):	7.814365220066478
Encrypted:	false
SSDEEP:	384:fbZaAb0yUMZ95IQRVAfobZCXLd/ZIFNHNY9tFiIleFwsQqH9:DZgySQjBShANa9tFiIle+sQw
MD5:	A2AA2B4620EC4C797042811C008D3B89
SHA1:	B23CE846CC395867F219C33C42A094197816B9A6
SHA-256:	FBCE541750335AE8C5BB4839F2D7EBCFC7B5224E0CE01B97C17EE89E6ACBBC80
SHA-512:	34B8032574C430C5639BAB431DA8BDEAD67819666728173787D4BBD3DFE6C9A48EE62F1172EDAC5D0C7B46455BE6954A82E9BFC996126922DC2854129D3741D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1083_Panel15_Mosaic_Item5_Stand.jpg?version=00530597-9619-2575-35f4-6d87092a5ab8
Preview:	JFIF.....!GS:-zi.Q...vi...T.EB*.E[.l7 ...a..@...+H.V.+.....AC.f.....PT..aR.-.W...@...1~h.....U...3.=nN...c.....".XT.po\$6.zO.!.+.8.....`(T...rD_y.T"...3....QR*.TB+....]...."R...8...X"...V.*..g...*EJ1.f...V.H.EJ..w....=.. .T.8.Y.....*V<..?w;..T"...T*V.*U.....8T....?@...V.H.+.....>..V.X.2...X....D".l.k.k.AR*...2...."(T...=..z....1.c...."+.W.....v@*V..F:..@..T"...Q]....i..Ua.1.b..V...*T.t...l.. ".TT.c....X..*..a...*Q:..T.Pc<...T..T..!t.<{..D".aP1.f....DT..TU.<..G..U.+..W....".."V..A...^..n..U...?....B..a...9.j.n..].XEQ..8.G.."....a.V..o].g..S./au.!D.*p....."...W.y...#.. .R7>...../.....EH.T..l!:=UU...U...p.....!+.7.....Tu.{..U.....9t.....a....v+...-t.3T@...X.Yt.....EH.....t/w;.."P..a..T+...D@"...T....

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\1083_Panel15_Mosaic_Item6_Blue[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 1084x400, frames 3
Category:	downloaded
Size (bytes):	6212
Entropy (8bit):	1.6100658993341477
Encrypted:	false
SSDEEP:	24:IK1h6A1aWwh82YSGjgh9V0hGT3TyJEumGumNG0jJdY3dK:y11LvnMh9GhGCJEdGdNVJp
MD5:	51AB8389477226C75A09B794182FAE41
SHA1:	39F40C7E3FB67F8744D0FC8D9D4862D67FDCC1D7
SHA-256:	724754E5EC6EBAD1B2A30240E7127FC39AD3622D8326AAF1ED80FBAEB05493D8
SHA-512:	54F3419DFB073F964588EAAC152A2A5BBB89083237EE31EEAC69B2CB86F1C421F2F8AE1217BB3A4369A12D74EF482EDA1F2B1EA581F727372F930E486DFCD6F1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1083_Panel15_Mosaic_Item6_Blue.jpg?version=b055c5ea-fc4e-ade1-57d1-79faffe1d713

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\1083_Panel15_Mosaic_Item6_Blue[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 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:a bout="" 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:F80924DA5CBB11EA88EEDBD181122FD0" xmpMM:InstanceID="xmp.iid:B56B8D7A5CBB11EA88EEDBD181122FD0" xmp:CreatorToo l="Adobe Photoshop 2020 Macintosh"> <xmpMM:DerivedFrom stRef:instanceID="8F6B98E30D2E75BCEAE1C4EA6B2EEB5C" stRef:documentID="8F6B98E30D2E75B CEAE1C4EA6B2EEB5C"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.....Adobe.d.....
----------	---

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\1920_Panel05_FeatureGroup_Included[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):	113867
Entropy (8bit):	7.982054439851882
Encrypted:	false
SSDEEP:	3072:sELN5aV7sH8XyYwEu6ut37dGM1ISdi+17IZKAGTaeyUSmN:1J5aV7w8lyNlup7dGAEG+zEpypl
MD5:	4BB468CA58FD0CF57328BB6A16C2066B
SHA1:	BC97F96DCB8F03D92F5E2148C2E8EF0F71D28DED
SHA-256:	26BC7EAB441EF30D0BAD4F4C35330E3763D827180ACFF021E9D0D04077223DE5
SHA-512:	CCCFDB7B3128C34A42C18341A0D579B4866753E04B3ED0D45B6F66BED0EBC0A30CF491D2E6E753EC30E4897C07AD4181441C995A3B0AA03C5DC0190310492F4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel05_FeatureGroup_Included.jpg?version=976539f8-3873-bee1-7def-175fd679d5e1
Preview:	JFIF.....&%C.s\.....e..7..&..P.C g...ms.#DHU..G.*.....d.Q..H.l.}.....}...+e.:A..L....R....5..}K..~.b.V..tz,...+y.z].m)4.M]1.H..Q....6#.H.D\$#5.9.s.{...G.M..#..[.....nN~.3[.6Y.&H.(c..1.....7B....b... ...Dt<h...Y\$#F..61...W\$MUUs....h.F.U]\$.O&q..a..}...s.X.)4+6FD.q..Lk..Q1....{d....T.k...vW..7..n....~...+TFD.....r.&..W9.D[.6..Ts.....R.....s.;j.)BI6d..q...66..x.....:g...v...i.. %.(9.;R....\$dJ+..5Dt~.....4...G...=y.Vhu-^F.]gZ..q>VK..7F.dQ...9.....+.7y8.(p.5.....X.'...\$nPdLb"..D...].p...Q9.PwN.m..\$.r...g..c.s.2.Y.N.'q.P.j....Q.PF.(...s....J.J ...%..l...M.s...ce.oe.r....*H.....r...W..9.+s.;3.U....\...G.s.8Q.e.i.....jt....\W9.9...mkd.l.....c.p.E...oP.....}....\$.r!c...3.#A.....S....

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\1920_Panel06_FeatureGroup_Gaming[1].jpg



Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1040x585, frames 3
Category:	downloaded
Size (bytes):	236876
Entropy (8bit):	7.990346898007754
Encrypted:	true
SSDEEP:	6144:oC640zybA8lcEkzIzRsYiDBiq6rvDhHfQBui6HHun:oC640zQA8qPlzRXd97DtfQBR6nun
MD5:	95027239609EC0AC49C3CC8E9DFDCCC
SHA1:	B0EAE8B25DA2F83749AA924AAE7339BB934CD383
SHA-256:	A3DF3A4F0D300279247AB64A8244A2643FE0098BD329A0C9B5D9638D39CA8F95
SHA-512:	676F0378D8AFOF9A776285B6ECCC13D82745CC0073C0A5FD21678BCE80533C0B756A194525748089623F1315CF1631084EC4C20A9480F6CF9101BECD67999B60
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel06_FeatureGroup_Gaming.jpg?version=67774c04-06d2-d24c-422f-d267d8c2963a
Preview:	JFIF.....Jf.9..3.....c.....6.r..R.s.:Y.n .R..R..uj.....l.O./vDQ..C.T.....y...C.a.g.).[C.....8u5t...UkZ~.Y...g.].;1].[Rh..L.7.=...5O..a.Wl.\$q.Mx5..u{.#S+xt..m@".0emHB.l.....`....6..z..c.t~..J."5V[...e:rl.y..... t_/yk.q.U..8.:m.g....H>k.....~.kF....Eck7....d.(.~.8[.~.8C.....Wx~Ko+...i.`.....8t.[j....@...%Y.N.....@u.CU..J.G..S.x~....e.%..?b..QE...eF.;[jo.H.[W.....`M.. m..%RU.X.....T...].M..C5.4m..A..="W....2...v.....a..f.W....].Cm.L.LV...2v..y~B...6...8.."f..Tf.3.O.....\.;W...L./..i.nMT.e...^T..d.]m.O.qaZ.YX^..Si....`d....N...S<..X..r.'.l.W...M.X.. .K'.gb.d+b.'X..n.....=A^..@...V..`...m.R...Y..-.....&B..a_@.j..wQ.k.....].....M.M3ut:~...-M.E.B...0..n...a.6.S....Ru...-.%d..D%U.

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\1920_Panel08_MultiFeature_Hearing[1].jpg



Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1600x600, frames 3
Category:	downloaded
Size (bytes):	227039
Entropy (8bit):	7.9916100283027385
Encrypted:	true
SSDEEP:	3072:Vyis4q1ezMo8aRkW8EQT/MiWgXCc5ljoK6hgNXmT/Uyb/wqMAMHTieegCM:V7lqE/FCEKWMljtKBNQ/UybNYzieR
MD5:	98299AEA9DAFAD68B31EB40001156FC1
SHA1:	FBDB274C3D2CD467DEE7786CF7B58FE244559CDE
SHA-256:	64430FA721809567410A52812A611C2A0CFA0A102D38E4A128EBA8AC8A3DCB44
SHA-512:	7ED1E25F9D1C8A801EB063CF04CCFB63F4615EC64A81812D7C4D055FB952F1EC6408579A7E24978EF35023A138336E0BE5BAC0BE5EB2C000DAC6E52F2CC655
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\1920_Panel08_MultiFeature_Hearing[1].jpg	
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel08_MultiFeature_Hearing.jpg?version=48d71b3d-1873-8a94-48cf-51b5004493b1
Preview:	JFIF.....X.@.....k.Z.....3.M}tH.....I.Z... ..g.=r....u}.C.....'.....O.....\$7qdQ..Z.=...y...r.3u.YT...EF.?E.E.a.6.f2..j...n...q.TZ.Ke...0]{...l...\$.HQ.....KJ[q.l..D. D.....f..].d.5...=m2...1C.....f....xB.Q....l.6...i.J^W.8.{ O...@.u.j.s...S./.8....2...s.j...., @.&}.....8z*-W.ojx.4.Z+{.J....\n..d...q+S..C.m...7L6f.(Ll.)V..^.....;W^..9.)..../a...'.c.....M...8.MW..YM.,M...@i.6...2w.{\Fu.oo:5<...p). f.....Jy.-.y.<mFa.s"6..h".r.vs....h`.}.g...j.l...u}6U.Ms&t.....a...\$.m.q...T..L.F...s.t.K.....^.....l...}.....7.J...)i....i.w....l...D(>.]V;..gU.....i.[^...c....m..bQJL.8.;nY.."X.}.5]. d.....uVv2.a.w...J.*l.\S..8kuKyF..Y..46.....dt...b...;.PD...E..".s...O.....y..eWf18j(.D...av.T.c.{

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\1920_Panel08_MultiFeature_Learning[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1600x600, frames 3
Category:	downloaded
Size (bytes):	154463
Entropy (8bit):	7.980540779560687
Encrypted:	false
SSDEEP:	3072:4Cr14cw74AJ6mASech9FpRt1D61ceWdYOA7T0yekQiMo45iNse+CqUoc+S:BRwPFechlP1+6dYOae3cKCH1
MD5:	FCE5785C7B2CD07CF4D4CCF714EDDE7C
SHA1:	BB47750929164429A011A023110459532325D7DD
SHA-256:	E3B14A3304DA30A76B5D30D6B717D18918792E0EF8C9B2BF1A60C6F30E54E7DB
SHA-512:	33B13ECAA533B366E42B9E46EBF84626ECABD58509A435AD795D6D8A99571F417AB4AB37F062A2B3E06831D8011D5DF8D6041A8028FB4C3DBF7C2ECAA1B9A8C3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel08_MultiFeature_Learning.jpg?version=dd0f5222-972f-3d6a-c4b1-8d1f3cf273c0
Preview:	JFIF.....X.@.....T.5.....Z.C2l.a.n.&..?l.;rkn.j.. ..=yy.....@.kZ...h...kCZ...hhk@kH.\$l\$.H...o:.....v.....r...;y.{.....".9.....q.....r.m.Zu..X.T*5....99".c3."..e..1W9?F..7zgn.*....x.....P..h.A.....45..5.kZ....5..@..... 5..B.....;l."v.G. 9.....F..gY.....& .k.x.Ty.}.3.....X_!.....[.].p.k?w.3O\$.kq.n.a....U.K...O.s:<uX.`].l.fG.....cCZ.1.445..4.....".4.....mM<.....a.....y..g3w).Xm... . { .G.3.T.K:~../.t.K.....tj=..u..8..5..".8...{.o.t..6.*....J..k..m..{.@.....c.kZ....5.4...H..Dq.....H.v/KOw....0F....Y.....n..k.U..^l.....>7..Pi>...{.}/.V...V.<..Q..^.....J.4....X..[.].s.v ..1.V.5lx.P^Ke.....h.....B..hk.....5...\$.^.....h.s.B?S[b.....?WO.l.d.4...W...;.....-Kls.^..0z

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\1920_Panel08_MultiFeature_Mobility[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1600x600, frames 3
Category:	downloaded
Size (bytes):	164044
Entropy (8bit):	7.9854058825476475
Encrypted:	false
SSDEEP:	3072:PTt3xNdtSq6s/zGCBKRtX3AshnVxXJyUx2Uf4jzLz+JvQfLstsMDkweWRMjyOmS9:PTffY+ojhnV3y82UfKHPZ+MLm6
MD5:	9C30CB9B4D52B8B57B260421BB813452
SHA1:	481E44056B658635D5F2122112637DF9616C54D7
SHA-256:	AD094954A7FFAF116311CB233FD50C5A9859A6ED43BF20D5FC5C564E1E0725DF
SHA-512:	C4D91EEF1F967F0BE228C0C254101E9FD04EF504ED754E750E6DA0D92FFCB06EA8FE16DE7CE54A2AA422738DE1BD9A7A441DC4D5C4947F1EAB2577DB6508D41
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel08_MultiFeature_Mobility.jpg?version=d6cee281-0b4a-7da7-45c1-9290b6842199
Preview:	JFIF.....X.@.....y-d.`;...\$.P.u.(H....^.....~.....>.. U@'.....l.....9.}. {.....g...b..k.F..T...L....P...\$.M./~..3.c@kU...*...aP.T5.^.....8.M.Y...G..i.N.6.....3.B..[{n...Q.Zr...=de*.NI.iw.WCp}....F...P.18...9z^...{.....3.c8.= {.... ...~..%l...z5..r.r.....U.N.....z..xpU...Ln.}.b4..ZC.....~.....B.h.r.1.G.eh.l.J.l.l.l.C.:g!...6..G.:K..{?Wtg'/f.c..j`..e9...}.g8.1.g9....={....&}.H.V.<1q7F.k....Lz.\)...t.....^V.Oh.'6. N8.i.f../).F....dm..z..he..q.R*b=tm..^FH.....p.W.0..1.}.(uZ...p~..n.^.....Z..{.3.'+...^}.G..e.{.}. {.....Y...Wc..E.8..{Y)D..s.6..n.0.4.&fl...;euc....m/%6ef0.Z.<W.&.....R.. ..?.....&l..j4.S...wL..^..N.....?g.."..@3=.....y..b8..g....{... c.v.W..+.*.1.W.<E. g1..Q`..M.?..._..cB...~cDk.ral(.Q.../.

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\1920_Panel08_MultiFeature_Neurodiversity[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1600x600, frames 3
Category:	downloaded
Size (bytes):	278723
Entropy (8bit):	7.986069001342278
Encrypted:	false
SSDEEP:	6144:FF/OC7PpRlbwldDyBRCgzDIGu2lQuO6+nLWB+RfZ78YUnRP:FFVPpRDgNyOmBmRns+RfhVURP
MD5:	A0378549FE18E517D0BB7DB89EF2ABA0
SHA1:	56CBB69087DB552D6931C75510314F19A422D472
SHA-256:	9CF00A82DB570C191B03AC3908FE04E42BFE31F2A0FA32675ED7F59E39259231
SHA-512:	14146F824EE237655E718AC754B2B0ACB49BBCA4B86656750E07D68BA8962C530F75662CCA9975093D14BCA153177D61DD4F6261035ED6BEC5C44B7620DE7DC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel08_MultiFeature_Neurodiversity.jpg?version=dd9094cf-5aed-e3ec-4c49-2f0ffb0131d1

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\1920_Panel08_MultiFeature_Neurodiversity[1].jpg	
Preview:	JFIF.....X.@.....js.F...Y....eK.X..b3x%V+...n lh!.&6k.r9#U...Bj....f.?..F...e...qp....-E3Q.z.V....\{.....\\$.Q.....?^A...}\.a..Q....is.]5..+E..^O....K.Ax.p.....V.cd\..ZU...J..`Y....1V.9r....%XGt.~fuQ...Tr.K.....S...#... (..._dWi..?.K..G..j.n...+X.ET.3.+i.O.....").Z..p.8K...l..lz;4..x...b.a..a*A...l..b.EU...{....XM+....;`'`*.....%C:&}.m.g.y-@.lk.....f....@RL.....+uX.`8....l[.SC.`.....>_. ...e.....i5...+j.Wh...E.....+...%\$.c.`..P.,z.Z...j...B["t.]KN.x..6h..E.L....T*)..vr.R.X...l.wycla..j..K.X..%s{.....#..h...z..8...q[YAT....q.d.s.Z.K.....T..Y...@.xF.Rk....3.....U...h...-Y .r.t.*V....TX]F.\$...wc..x...X-l...r...q...~..2.yo..lx.2.4N.<..s.!aRk...W#X.z...W!.../..W.

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\1920_Panel08_MultiFeature_Vision[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1600x600, frames 3
Category:	downloaded
Size (bytes):	146147
Entropy (8bit):	7.984535233340891
Encrypted:	false
SSDEEP:	3072:T6avn/O69eKkentiVUsGwnYzE6XGkVmLzh4K+Lg+8KDxIO5UEnK1kc:THn/O68KZiqwnaNWkVLg+8UOEnK1kc
MD5:	B0C5C3E44C5CF2A751CAF27B9B5B6D37
SHA1:	B313682B9EDA9EC8B78774626BD1357A8FA8678D
SHA-256:	6524F98BEC9612ED758ED3883BAB60171AC10D4E833D6A53A106573EE7520C4C
SHA-512:	8CFD6817BF114AB176B8E1E2DAA22AEC1BD18F26B640F3CE1B79AC9BA44A1466E39F75918C0B7C47061FE663D92BB2D6E62F6BF2086E42423BFAAFC06A2596D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel08_MultiFeature_Vision.jpg?version=2e286003-dc42-a343-06c7-a89bf41afc60
Preview:	JFIF.....X.@.....R....IT..nM.....^e..[O-C...DB. ...N.....7..Tg.!AW.3Q.@i!..B..?G.A...U.m..Y\$!...X8.....'6NJq.RIA.q;\$;..NWZh5.)y,,:;YZ8p*k+..(...#...Rd...J...=2tzjH...cuQ..q...U...&K..JH.....m.....%...5..m.....J)+A. .ED..D..UPY..yL.T..3...-L.d....3IM..mk...;o.....9.9{.....E]t8....". (. "#M5..^...LF.<.....q.i>5DRx.Y...[....A.w**..H.....2.(...U...5.^.....I9.7^..W?"..S..rT1\Ta.5.T..<'.)"=-..m.....^v. ..g..U.Qj...d.l...M... "r.H..v~..7}...+ " ".....>K...&.lwc2d....>zu...\$.a...m.]..7%N.Cl..YC.._#j%.....\..X.@.[.4.u...2t"...E6.^e...Y!_G..xq.v1.2Y..P.....1..yt.l..5.lmk.....u.. ...^l..S.K..T.W....1...#...*#m+.J.(.#.<k...&...Y.V..C..z.Q.Gz.>z..-..2d.<n.....^O.A.....21i.[...DIU...o...u.g.

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\1920_Panel10_4Up_Ideas[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 358x201, frames 3
Category:	downloaded
Size (bytes):	26797
Entropy (8bit):	7.9702343818998465
Encrypted:	false
SSDEEP:	768;j9g2HNjMjNt7tf5xAqTKQWYLCEmAeUU13:xaBNVoQN1XAeUU13
MD5:	7F13D5037F3845E797123874BCC2122F
SHA1:	FE8E8EA5160C7D4EC61EBB8B0ABCE3157565D8A8
SHA-256:	93ED25E616450B512FC1038805238C83669D1006CA7B3FBEC2A811DCDA05211A
SHA-512:	F18F05318C805DE99EED7839856981A5A22C366102B19F498CC210CE71896C75855B77B5B528811D2169C51AA2AED3EB1C6CEBF7504E1089DAA282FD12313854
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel10_4Up_Ideas.jpg?version=4aa4ad31-1581-9d76-ef2f-e9ebe3f8e42c
Preview:	JFIF.....f.....k...b.r.....~]@*.....c...C.I ...teso..D..3..*M.....'6...&_y\$X.krX.=kt'[B.....z...X[n.6..F.?k...@..jp.k.d.....&/.....j'...K....^.....&...y....lx.....^y.z..x.....5.5.w.mL...p.N...l..>g.....[.j].....u.....]g 9.....k...d.\N..j'...F...".K_J..63...&_ _B%v..S.....(l....%m.0...kc.....S....hr...f.o...u...F.FyR.=.....#; .j..i.t..#n.g.4FWf...E..^N.....*"...Z...j3+OO9o.+m..+b..M.....+.. t.....yz...)FyqpX.L5tw.....n...`..F.6...7X..~...+k..P#T....6.....u.....rj...>Sjt..u.%%..._1...&.z.i.....t4.[.....M.J]"R...oru0.....f...f....k.Ws...lru0..uk...8e.p....6..B6...ru0..m... _...M.W..t....L..uk.'u.+...l..._...y':.....y'}.!.....*P.m...8...2.....z

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\1x1clear[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.122191481864228
Encrypted:	false
SSDEEP:	3:CUTxls/1h:/7IU/
MD5:	F8614595FBA50D96389708A4135776E4
SHA1:	D456164972B508172CEE9D1CC06D1EA35CA15C21
SHA-256:	7122DE322879A654121EA250AEAC94BD9993F914909F786C98988ADB0A25D5D
SHA-512:	299A7712B27C726C681E42A8246F8116205133DBE15D549F8419049DF3FCFDAB143E9A29212A2615F73E31A1EF34D1F6CE0EC093ECEAD037083FA40A075819D2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/_h/9be151e5/coreui.statics/images/1x1clear.gif
Preview:	GIF89a.....!.....D.;

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\50-f1e180[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	133618
Entropy (8bit):	5.224613249025047
Encrypted:	false
SSDEEP:	3072:1f/HuFVppxvleJ0i9d1EwgXA9JKi5DCE5n:1f/Hu/FlERxn
MD5:	0405301724624162B6706F1AB465531F
SHA1:	1C034383716BCE493E28BFF0DD2C27F049CC558
SHA-256:	A5DD3C05EFED81BBF60B618C07A07746F030147590EE0EDD74459AC4E53955FD
SHA-512:	9DB1E61D3B0AED73F7A64D0344E432AEAAAB057655CFEB040348FA876693E618A434D63727F1E4AA1118276740C7102FD412637B46752665B78EB3C81A53915A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketing/sites-eus-prod/shell/_scrft/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-c07ea1/29-1ec5a9/23-c64e70/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/79-499886/7e-cda2d3/b2-7087f0/e5-08f1c0/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/50-f1e180?ver=2.0&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+=1)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\NetCache\IE\MEEXW4H4\Blog-high-contrast[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 20 x 20, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1204
Entropy (8bit):	6.620936303411696
Encrypted:	false
SSDEEP:	24:11hSWwx82lY2T3v4VgugAyJ3VmCQT+2eGUwnXAKuz3qVEZ+Lc:bBNn2z4wJ30CBrwQKuYnc
MD5:	C0158ABD85F9C71344A95631C5C5B80E
SHA1:	21456B3E187FA8262BDDF87629F9E8E2252BC10
SHA-256:	FD351788DDD8A404E52617F00DCA9CA802D2FBD642D713133116E899A9E322AE
SHA-512:	5645CDB367444E5FC7657E78622041B85B7D0D2D54349E85EC429AB53683C111702ED1A2A877E87FE0AA830C1D323CAA16CEE17AF5D7A2D3802C2117EE3A059
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketing/sites-neu-prod/_h/fa9a23e2/office.testdrive/images/social/Blog-high-contrast.png
Preview:	.PNG.....IHDR.....tEXtSoftware.Adobe ImageReadyq.e<...%iTXtXML:com.adobe.xmp.....<?xpacket begin=" " id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta ta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 6.0-c002 79.164488, 2020/07/10-22:06:53 " ><rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xa p/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop 22.0 (Macintosh)" xmpMM:InstanceID="xmp.iid:E0DB8A6530A511EBB51D8748B1217C9D" xmp MM:DocumentID="xmp.did:E0DB8A6630A511EBB51D8748B1217C9D"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:3878F5F030A511EBB51D8748B1217C9D" stRef:documentID="xmp.did:E0DB8A6430A511EBB51D8748B1217C9D"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end=" " ?>d.....%IDATx..N.1..q....08.g .Br2...77..W...).....3.\$:.....f...^..M..J.p...8.....\..R.<GQ^..Q.TF.cl.B..4lW.....#.a.e

Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 132

- 53 (DNS)
- 443 (HTTPS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 19:07:40.584309101 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:40.585170031 CET	49708	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:40.730359077 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:40.730545044 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:40.730618954 CET	443	49708	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:40.730751038 CET	49708	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:40.740483046 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:40.740948915 CET	49708	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:40.887480974 CET	443	49708	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:40.887547016 CET	443	49708	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:40.887582064 CET	443	49708	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:40.887620926 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:40.887661934 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:40.887702942 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:40.887732983 CET	49708	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:40.887789965 CET	49708	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:40.887789965 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:40.887985945 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:40.937406063 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:40.937485933 CET	49708	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:40.943574905 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.083667994 CET	443	49708	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.083817959 CET	49708	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.084131002 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.084300995 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.143759966 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.213040113 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.213082075 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.213104010 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.213125944 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.213146925 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.213170052 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.213172913 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.213197947 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.213217974 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.213222980 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.213241100 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.213260889 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.213280916 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.213303089 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.213318110 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.213324070 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.213352919 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.213375092 CET	443	49707	52.104.14.25	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 19:07:41.213383913 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.213421106 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.213429928 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.213490009 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.358593941 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.358665943 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.358719110 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.358730078 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.358762980 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.358788013 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.358788013 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.358845949 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.358855963 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.358897924 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.358913898 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.358958960 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.358959913 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.359015942 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.359020948 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.359067917 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.359075069 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.359118938 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.359129906 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.359179974 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.377671957 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.421328068 CET	49708	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.423077106 CET	49709	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.424002886 CET	49710	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.424887896 CET	49711	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.527942896 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.528003931 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.528024912 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.528060913 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.528074980 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.528120041 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.528126955 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.528177023 CET	443	49707	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.528204918 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.528243065 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.531174898 CET	49707	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.570790052 CET	443	49708	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.570859909 CET	443	49708	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.570920944 CET	443	49708	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.570959091 CET	49708	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.570982933 CET	443	49708	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.570990086 CET	49708	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.571007013 CET	49708	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.571032047 CET	443	49708	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.571053982 CET	49708	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.571072102 CET	443	49710	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.571093082 CET	49708	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.571113110 CET	443	49709	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.571207047 CET	49709	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.571400881 CET	49710	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:07:41.573024988 CET	443	49711	52.104.14.25	192.168.2.3
Jan 13, 2021 19:07:41.573128939 CET	49711	443	192.168.2.3	52.104.14.25

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 19:07:35.050479889 CET	49199	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:07:35.098555088 CET	53	49199	8.8.8.8	192.168.2.3
Jan 13, 2021 19:07:35.864253044 CET	50620	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:07:35.912478924 CET	53	50620	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 19:07:36.808634996 CET	64938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:07:36.856781960 CET	53	64938	8.8.8.8	192.168.2.3
Jan 13, 2021 19:07:38.093692064 CET	60152	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:07:38.141859055 CET	53	60152	8.8.8.8	192.168.2.3
Jan 13, 2021 19:07:39.128873110 CET	57544	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:07:39.185657024 CET	53	57544	8.8.8.8	192.168.2.3
Jan 13, 2021 19:07:39.480715036 CET	55984	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:07:39.541541100 CET	53	55984	8.8.8.8	192.168.2.3
Jan 13, 2021 19:07:40.477420092 CET	64185	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:07:40.518635035 CET	65110	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:07:40.525587082 CET	53	64185	8.8.8.8	192.168.2.3
Jan 13, 2021 19:07:40.575287104 CET	53	65110	8.8.8.8	192.168.2.3
Jan 13, 2021 19:07:41.356848001 CET	58361	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:07:41.405311108 CET	53	58361	8.8.8.8	192.168.2.3
Jan 13, 2021 19:07:41.416763067 CET	63492	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:07:41.445008993 CET	60831	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:07:41.477813005 CET	53	63492	8.8.8.8	192.168.2.3
Jan 13, 2021 19:07:41.505167007 CET	53	60831	8.8.8.8	192.168.2.3
Jan 13, 2021 19:07:42.931593895 CET	60100	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:07:42.982538939 CET	53	60100	8.8.8.8	192.168.2.3
Jan 13, 2021 19:07:44.050261974 CET	53195	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:07:44.108877897 CET	53	53195	8.8.8.8	192.168.2.3
Jan 13, 2021 19:07:44.866116047 CET	50141	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:07:44.917190075 CET	53	50141	8.8.8.8	192.168.2.3
Jan 13, 2021 19:07:53.534497023 CET	53023	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:07:53.592684984 CET	53	53023	8.8.8.8	192.168.2.3
Jan 13, 2021 19:07:53.637286901 CET	49563	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:07:53.698611021 CET	53	49563	8.8.8.8	192.168.2.3
Jan 13, 2021 19:07:56.842037916 CET	51352	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:07:57.055022955 CET	53	51352	8.8.8.8	192.168.2.3
Jan 13, 2021 19:07:58.604151964 CET	59349	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:07:58.652205944 CET	53	59349	8.8.8.8	192.168.2.3
Jan 13, 2021 19:07:58.806267977 CET	57084	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:07:58.854187012 CET	53	57084	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:02.573910952 CET	58823	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:02.622155905 CET	53	58823	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:03.545334101 CET	57568	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:03.593427896 CET	53	57568	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:09.485080004 CET	50540	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:09.486313105 CET	54366	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:09.535916090 CET	53	50540	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:09.544862032 CET	53	54366	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:10.060379028 CET	53034	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:10.115405083 CET	57762	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:10.135166883 CET	53	53034	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:10.163289070 CET	53	57762	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:10.487751007 CET	50540	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:10.538671970 CET	53	50540	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:11.130992889 CET	57762	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:11.179174900 CET	53	57762	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:11.489741087 CET	50540	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:11.540616989 CET	53	50540	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:12.144165993 CET	57762	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:12.192080975 CET	53	57762	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:13.687354088 CET	50540	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:13.747009993 CET	53	50540	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:14.160120010 CET	57762	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:14.208194017 CET	53	57762	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:14.928297997 CET	55435	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:14.991199017 CET	53	55435	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:15.292684078 CET	50713	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:15.353358984 CET	53	50713	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:15.920608997 CET	56132	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:15.939567089 CET	58987	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 19:08:15.941605091 CET	56579	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:15.954833984 CET	60633	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:15.975034952 CET	61292	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:15.979643106 CET	53	56132	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:15.997364998 CET	53	58987	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:15.999051094 CET	63619	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:15.999234915 CET	53	56579	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:16.013470888 CET	53	60633	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:16.046458960 CET	53	61292	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:16.057018995 CET	53	63619	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:17.700537920 CET	50540	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:17.751575947 CET	53	50540	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:17.863943100 CET	64938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:17.927277088 CET	53	64938	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:18.180713892 CET	57762	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:18.237009048 CET	53	57762	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:19.488528013 CET	61946	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:19.547692060 CET	53	61946	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:22.310892105 CET	64910	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:22.368248940 CET	53	64910	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:23.858807087 CET	52123	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:23.919699907 CET	53	52123	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:24.273401022 CET	56130	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:24.354598045 CET	53	56130	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:25.024153948 CET	56338	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:25.072063923 CET	53	56338	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:25.182867050 CET	59420	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:25.230642080 CET	53	59420	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:25.987718105 CET	58784	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:25.990350962 CET	63978	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:26.034667015 CET	62938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:26.045341015 CET	53	58784	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:26.048094988 CET	53	63978	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:26.074110031 CET	55708	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:26.093657017 CET	53	62938	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:26.132977962 CET	53	55708	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:29.285022020 CET	56803	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:29.356257915 CET	53	56803	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:32.333410978 CET	57145	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:32.390088081 CET	53	57145	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:33.094235897 CET	55359	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:33.153605938 CET	53	55359	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:35.895749092 CET	58306	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:36.885787010 CET	58306	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:37.948498011 CET	58306	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:38.006196022 CET	53	58306	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:38.301008940 CET	64124	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:38.358385086 CET	53	64124	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:38.608342886 CET	49361	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:38.668616056 CET	53	49361	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:44.358530045 CET	63150	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:44.363460064 CET	53279	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:44.406431913 CET	53	63150	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:44.424333096 CET	53	53279	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:45.167293072 CET	56881	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:45.225138903 CET	53	56881	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:45.357218981 CET	63150	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:45.413220882 CET	53	63150	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:46.370955944 CET	63150	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:46.418770075 CET	53	63150	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:48.387659073 CET	63150	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:48.405255079 CET	53642	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:48.413053036 CET	55667	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:48.446201086 CET	53	63150	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 19:08:48.463084936 CET	53	53642	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:48.475826979 CET	53	55667	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:50.028270006 CET	54833	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:50.100707054 CET	53	54833	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:52.433778048 CET	63150	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:52.481936932 CET	53	63150	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:56.422687054 CET	62476	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:56.481805086 CET	53	62476	8.8.8.8	192.168.2.3
Jan 13, 2021 19:08:56.849817991 CET	49705	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:08:56.897691011 CET	53	49705	8.8.8.8	192.168.2.3
Jan 13, 2021 19:09:02.194463015 CET	61477	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:09:02.197520018 CET	61633	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:09:02.200884104 CET	55949	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:09:02.211352110 CET	49342	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:09:02.211688042 CET	57601	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:09:02.215322018 CET	56253	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:09:02.228743076 CET	49667	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:09:02.235626936 CET	55439	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:09:02.253674984 CET	53	61633	8.8.8.8	192.168.2.3
Jan 13, 2021 19:09:02.261501074 CET	53	55949	8.8.8.8	192.168.2.3
Jan 13, 2021 19:09:02.264096975 CET	53	61477	8.8.8.8	192.168.2.3
Jan 13, 2021 19:09:02.271672964 CET	53	49342	8.8.8.8	192.168.2.3
Jan 13, 2021 19:09:02.272027016 CET	53	57601	8.8.8.8	192.168.2.3
Jan 13, 2021 19:09:02.275444984 CET	53	56253	8.8.8.8	192.168.2.3
Jan 13, 2021 19:09:02.286447048 CET	53	49667	8.8.8.8	192.168.2.3
Jan 13, 2021 19:09:02.293093920 CET	53	55439	8.8.8.8	192.168.2.3
Jan 13, 2021 19:09:21.140670061 CET	57069	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:09:21.201721907 CET	53	57069	8.8.8.8	192.168.2.3
Jan 13, 2021 19:09:42.157737017 CET	57659	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:09:42.207449913 CET	53	57659	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 19:07:40.518635035 CET	192.168.2.3	8.8.8.8	0x69e5	Standard query (0)	cmrinsure-my.sharepoint.com	A (IP address)	IN (0x0001)
Jan 13, 2021 19:07:41.445008993 CET	192.168.2.3	8.8.8.8	0xf400	Standard query (0)	spoprod-a.akamaihd.net	A (IP address)	IN (0x0001)
Jan 13, 2021 19:07:53.534497023 CET	192.168.2.3	8.8.8.8	0x2426	Standard query (0)	cdn.onenote.net	A (IP address)	IN (0x0001)
Jan 13, 2021 19:07:56.842037916 CET	192.168.2.3	8.8.8.8	0x880e	Standard query (0)	cmrinsure-my.sharepoint.com	A (IP address)	IN (0x0001)
Jan 13, 2021 19:08:15.920608997 CET	192.168.2.3	8.8.8.8	0xdd68	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Jan 13, 2021 19:08:15.975034952 CET	192.168.2.3	8.8.8.8	0x23cb	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)
Jan 13, 2021 19:08:26.074110031 CET	192.168.2.3	8.8.8.8	0x1629	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)
Jan 13, 2021 19:08:32.333410978 CET	192.168.2.3	8.8.8.8	0xe98f	Standard query (0)	logincdn.microsoft.com	A (IP address)	IN (0x0001)
Jan 13, 2021 19:08:33.094235897 CET	192.168.2.3	8.8.8.8	0xdc21	Standard query (0)	aka.ms	A (IP address)	IN (0x0001)
Jan 13, 2021 19:08:45.167293072 CET	192.168.2.3	8.8.8.8	0xe579	Standard query (0)	amp.azure.net	A (IP address)	IN (0x0001)
Jan 13, 2021 19:08:48.413053036 CET	192.168.2.3	8.8.8.8	0xcaaa	Standard query (0)	assets.adobe.com	A (IP address)	IN (0x0001)
Jan 13, 2021 19:08:50.028270006 CET	192.168.2.3	8.8.8.8	0x538e	Standard query (0)	offertooldataprod.blob.core.windows.net	A (IP address)	IN (0x0001)
Jan 13, 2021 19:08:56.422687054 CET	192.168.2.3	8.8.8.8	0x35c	Standard query (0)	www.xbox.com	A (IP address)	IN (0x0001)
Jan 13, 2021 19:09:02.194463015 CET	192.168.2.3	8.8.8.8	0x1e00	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)
Jan 13, 2021 19:09:02.200884104 CET	192.168.2.3	8.8.8.8	0xb63c	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)
Jan 13, 2021 19:09:02.211352110 CET	192.168.2.3	8.8.8.8	0xc6b2	Standard query (0)	statics-wicrosoft.onestore.ms	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 19:09:02.215322018 CET	192.168.2.3	8.8.8.8	0x6d10	Standard query (0)	statics-eu.s.onestore.ms	A (IP address)	IN (0x0001)
Jan 13, 2021 19:09:02.228743076 CET	192.168.2.3	8.8.8.8	0xdec8	Standard query (0)	statics-ea.s.onestore.ms	A (IP address)	IN (0x0001)
Jan 13, 2021 19:09:02.235626936 CET	192.168.2.3	8.8.8.8	0xa0e9	Standard query (0)	statics-neu.onestore.ms	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 19:07:40.575287104 CET	8.8.8.8	192.168.2.3	0x69e5	No error (0)	cmrinsure-my.sharepoint.com	cmrinsure.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:07:40.575287104 CET	8.8.8.8	192.168.2.3	0x69e5	No error (0)	cmrinsure.sharepoint.com	698-ipv4e.clump.prod.aart.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:07:40.575287104 CET	8.8.8.8	192.168.2.3	0x69e5	No error (0)	698-ipv4e.clump.prod.aart.sharepoint.com	18980-ipv4e.farm.prod.aart.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:07:40.575287104 CET	8.8.8.8	192.168.2.3	0x69e5	No error (0)	18980-ipv4e.farm.prod.aart.sharepoint.com	18980-ipv4.farm.prod.aart.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:07:40.575287104 CET	8.8.8.8	192.168.2.3	0x69e5	No error (0)	18980-ipv4.farm.prod.aart.sharepoint.com		52.104.14.25	A (IP address)	IN (0x0001)
Jan 13, 2021 19:07:41.505167007 CET	8.8.8.8	192.168.2.3	0xf400	No error (0)	spoprod-a.akamaihd.net	spoprod-a.akamaihd.net.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:07:53.592684984 CET	8.8.8.8	192.168.2.3	0x2426	No error (0)	cdn.onenote.net	cdn.onenote.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:07:57.055022955 CET	8.8.8.8	192.168.2.3	0x880e	No error (0)	cmrinsure-my.sharepoint.com	cmrinsure.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:07:57.055022955 CET	8.8.8.8	192.168.2.3	0x880e	No error (0)	cmrinsure.sharepoint.com	698-ipv4e.clump.prod.aart.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:07:57.055022955 CET	8.8.8.8	192.168.2.3	0x880e	No error (0)	698-ipv4e.clump.prod.aart.sharepoint.com	18980-ipv4e.farm.prod.aart.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:07:57.055022955 CET	8.8.8.8	192.168.2.3	0x880e	No error (0)	18980-ipv4e.farm.prod.aart.sharepoint.com	18980-ipv4.farm.prod.aart.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:07:57.055022955 CET	8.8.8.8	192.168.2.3	0x880e	No error (0)	18980-ipv4.farm.prod.aart.sharepoint.com		52.104.14.25	A (IP address)	IN (0x0001)
Jan 13, 2021 19:07:58.652205944 CET	8.8.8.8	192.168.2.3	0xf7a8	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:08:15.979643106 CET	8.8.8.8	192.168.2.3	0xdd68	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:08:16.046458960 CET	8.8.8.8	192.168.2.3	0x23cb	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:08:24.354598045 CET	8.8.8.8	192.168.2.3	0x3aea	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:08:26.093657017 CET	8.8.8.8	192.168.2.3	0xf940	No error (0)	consentdeliveryfd.azurefd.net	star-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:08:26.132977962 CET	8.8.8.8	192.168.2.3	0x1629	No error (0)	mem.gfx.ms	cdn.account.microsoft.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:08:32.390088081 CET	8.8.8.8	192.168.2.3	0xe98f	No error (0)	logincdn.msauth.net	lgincdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:08:32.390088081 CET	8.8.8.8	192.168.2.3	0xe98f	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 19:08:33.153605938 CET	8.8.8.8	192.168.2.3	0xdc21	No error (0)	aka.ms		23.211.149.25	A (IP address)	IN (0x0001)
Jan 13, 2021 19:08:45.225138903 CET	8.8.8.8	192.168.2.3	0xe579	No error (0)	amp.azure.net	160c1.wpc.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:08:48.475826979 CET	8.8.8.8	192.168.2.3	0xcaaa	No error (0)	assets.adobedtm.com	cn-assets.adobedtm.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:08:50.100707054 CET	8.8.8.8	192.168.2.3	0x538e	No error (0)	offertooldataprod.blob.core.windows.net	blob.bl6prdstr14a.store.core.windows.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:08:50.100707054 CET	8.8.8.8	192.168.2.3	0x538e	No error (0)	blob.bl6prdstr14a.store.core.windows.net		52.239.152.74	A (IP address)	IN (0x0001)
Jan 13, 2021 19:08:56.481805086 CET	8.8.8.8	192.168.2.3	0x35c	No error (0)	www.xbox.com	www.xbox.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:09:02.261501074 CET	8.8.8.8	192.168.2.3	0xb63c	No error (0)	mem.gfx.ms	cdn.account.microsoft.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:09:02.264096975 CET	8.8.8.8	192.168.2.3	0x1e00	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:09:02.271672964 CET	8.8.8.8	192.168.2.3	0xc6b2	No error (0)	statics-wcus.onestore.ms	statics.onestore.ms.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:09:02.275444984 CET	8.8.8.8	192.168.2.3	0x6d10	No error (0)	statics-eus.onestore.ms	statics.onestore.ms.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:09:02.286447048 CET	8.8.8.8	192.168.2.3	0xdec8	No error (0)	statics-eas.onestore.ms	statics.onestore.ms.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:09:02.293093920 CET	8.8.8.8	192.168.2.3	0xa0e9	No error (0)	statics-neu.onestore.ms	statics.onestore.ms.edgekey.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 13, 2021 19:08:32.474028111 CET	192.229.221.185	443	192.168.2.3	49784	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jul 20 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Tue Jul 20 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2013 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 13, 2021 19:08:32.476969004 CET	192.229.221.185	443	192.168.2.3	49783	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	Mon Jul 20 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Tue Jul 20 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2006 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jan 13, 2021 19:08:33.244740963 CET	23.211.149.25	443	192.168.2.3	49786	CN=go.microsoft.com, OU=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft IT TLS CA 5, OU=Microsoft IT, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US	CN=Microsoft IT TLS CA 5, OU=Microsoft IT, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Sep 06 21:37:21 CEST 2019 Fri May 20 14:53:03 CEST 2016	Mon Sep 06 21:37:21 CEST 2021 Mon May 20 14:53:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Microsoft IT TLS CA 5, OU=Microsoft IT, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri May 20 14:53:03 CEST 2016	Mon May 20 14:53:03 CEST 2024		
Jan 13, 2021 19:08:33.247173071 CET	23.211.149.25	443	192.168.2.3	49785	CN=go.microsoft.com, OU=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft IT TLS CA 5, OU=Microsoft IT, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US	CN=Microsoft IT TLS CA 5, OU=Microsoft IT, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Sep 06 21:37:21 CEST 2019 Fri May 20 14:53:03 CEST 2016	Mon Sep 06 21:37:21 CEST 2021 Mon May 20 14:53:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Microsoft IT TLS CA 5, OU=Microsoft IT, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri May 20 14:53:03 CEST 2016	Mon May 20 14:53:03 CEST 2024		

Code Manipulations

Statistics

Behavior

- iexplore.exe
- iexplore.exe
- dllhost.exe
- explorer.exe
- iexplore.exe

 Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5364 Parent PID: 792

General

Start time:	19:07:38
Start date:	13/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff717c80000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Registry Activities

Key Path	Completion	Count	Source Address	Symbol
----------	------------	-------	----------------	--------

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
----------	------	------	------	------------	-------	----------------	--------

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

Analysis Process: iexplore.exe PID: 1064 Parent PID: 5364

General	
Start time:	19:07:39
Start date:	13/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5364 CREDAT:17410 /prefetch:2
Imagebase:	0xe30000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path				Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--	--	--	--------	------------	---------	------------	-------	----------------	--------

File Path			Offset	Length	Value		Ascii		Completion	Count	Source Address	Symbol
-----------	--	--	--------	--------	-------	--	-------	--	------------	-------	----------------	--------

File Path					Offset		Length	Completion	Count	Source Address	Symbol
-----------	--	--	--	--	--------	--	--------	------------	-------	----------------	--------

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
----------	------	------	------	------------	-------	----------------	--------

Analysis Process: dllhost.exe PID: 2168 Parent PID: 792

General	
Start time:	19:07:56
Start date:	13/01/2021
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Analysis Process: explorer.exe PID: 3388 Parent PID: 2168

General	
Start time:	19:07:57
Start date:	13/01/2021
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

Analysis Process: iexplore.exe PID: 2788 Parent PID: 5364

General

Start time:	19:08:12
Start date:	13/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5364 CREDAT:17418 /prefetch:2
Imagebase:	0xe30000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access			Attributes	Options	Completion	Count	Source Address	Symbol
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol	
File Path	Offset				Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly

Code Analysis