ID: 339264
Cookbook: browseurl.jbs
Time: 19:10:07
Date: 13/01/2021
Version: 31.0.0 Red Diamond

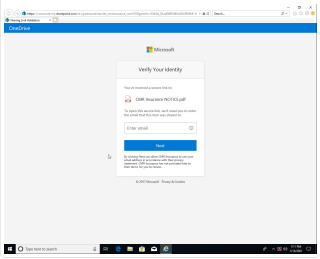
Table of Contents

Table of Contents 2
Analysis Report https://cmrinsure-my.sharepoint.com:443/:b:/g/personal/seccles_cmrinsurance_com/EXDgzrrmhc1GnNui_DLzzBkBEUB0mDlJ3B08lrE-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 9
Contacted IPs 15
Public 15
Private 15
General Information 16
Simulations 18
Behavior and APIs 18
Joe Sandbox View / Context 18
IPs 18
Domains 18
ASN 18
JA3 Fingerprints 18
Dropped Files 18
Created / dropped Files 18
Static File Info 52
No static file info 52
Network Behavior 52
Network Port Distribution 52
TCP Packets 52
UDP Packets 54
DNS Queries 56
DNS Answers 57
HTTPS Packets 59
Code Manipulations 60
Statistics 60
Behavior 60
System Behavior 60
Analysis Process: iexplore.exe PID: 3352 Parent PID: 792 60
General 60
File Activities 61
Registry Activities 61
Analysis Process: iexplore.exe PID: 2436 Parent PID: 3352 61
General 61
File Activities 61
Registry Activities 61
Analysis Process: dllhost.exe PID: 2148 Parent PID: 792 61
General 61
File Activities 62
Analysis Process: explorer.exe PID: 3388 Parent PID: 2148 62
General 62
File Activities 62
Analysis Process: iexplore.exe PID: 4316 Parent PID: 3352 62
General 62
File Activities 62
Registry Activities 63
Disassembly 63
Code Analysis 63

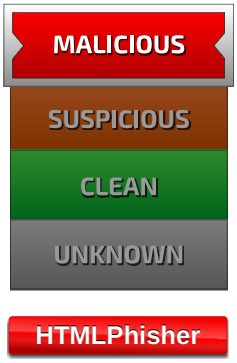
Analysis Report https://cmrinsure-my.sharepoint.com:4…

Overview

General Information

Sample URL:	https://cmrinsure-my.sharepoint.com:443/:b:/g/personal/seccles_cmrinsurance...urance_com/EXDgzrrmhc1GnNui_DLzzBkBEUB0mDlJ3B08lrE-XQmbmg?e=4%3avE67Ot&at=9
Analysis ID:	339264
Most interesting Screenshot:	

Detection

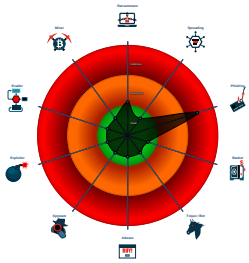


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 3352 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 2436 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3352 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 4316 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3352 CREDAT:17418 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- dllhost.exe (PID: 2148 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

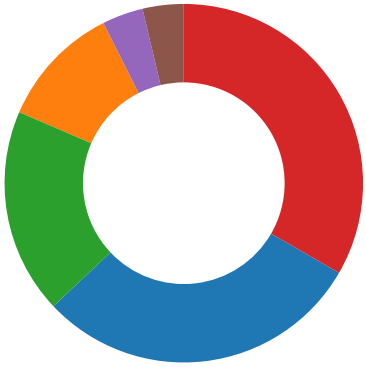
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\EXDgzrrmhc1GnNui_DLzzBkBEUB0mDlJ3B08lrE-XQmbmg[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

Phishing:

Yara detected HtmlPhish_10

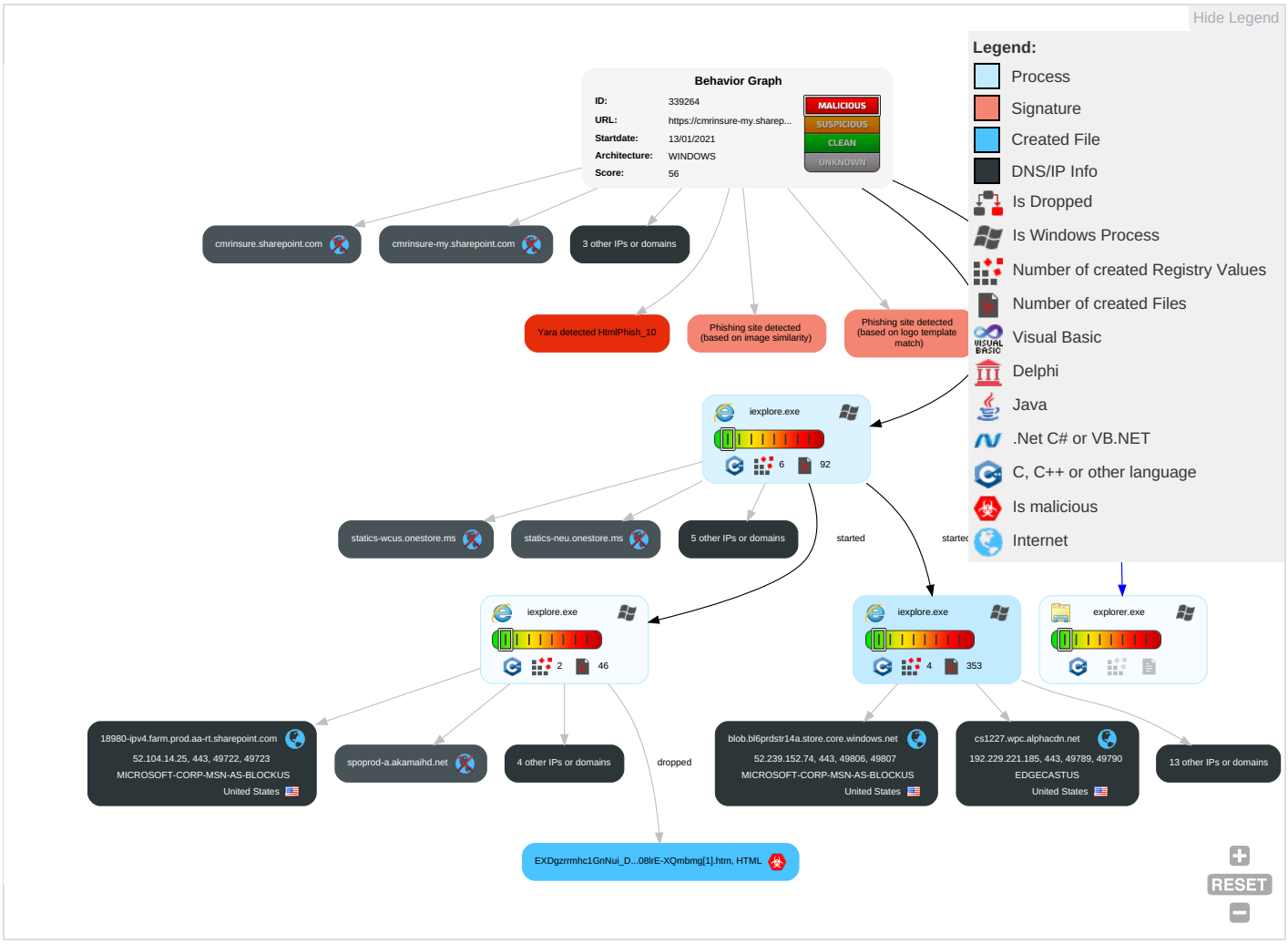
Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

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

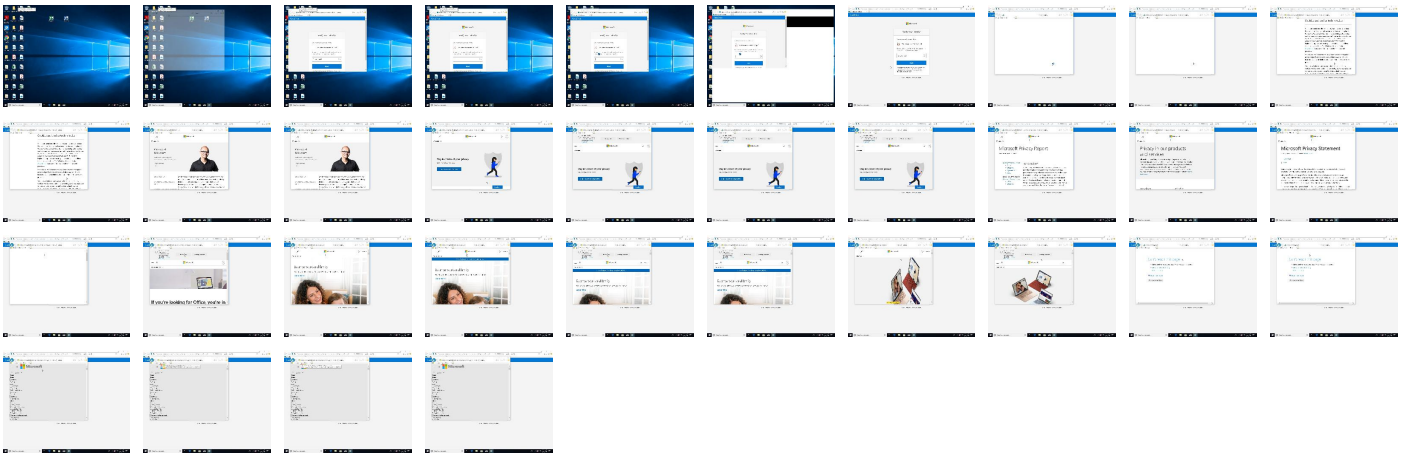
Behavior Graph

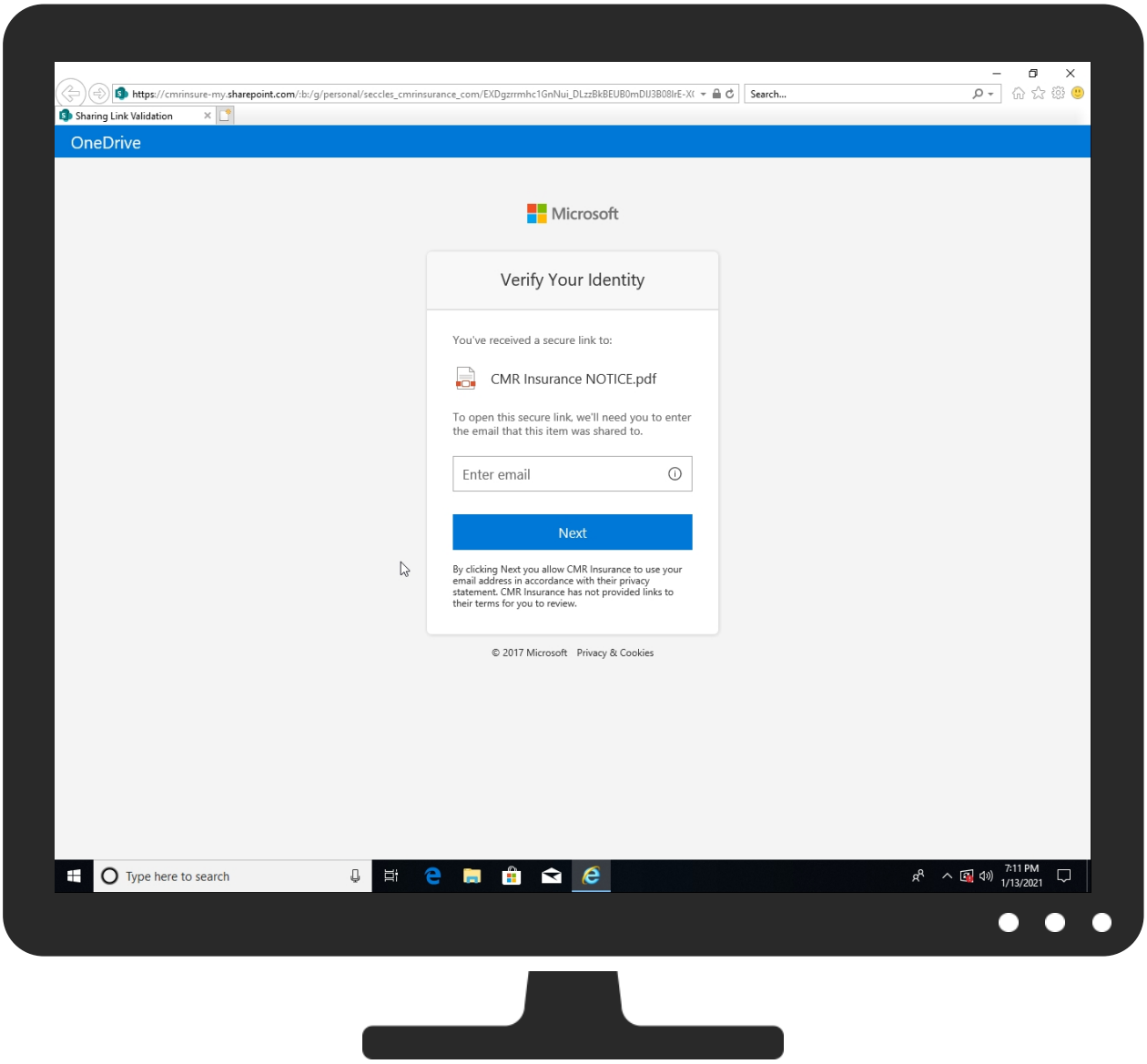


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://cmrinsure-my.sharepoint.com:443/:b:/g/personal/seccles_cmrinsurance_com/EXDgzrrmhc1GnNui_DLzzBkBEUB0mDlJ3B08lrE-XQmbmg?e=4%3avE67Ot&at=9	0%	Virustotal		Browse
http://https://cmrinsure-my.sharepoint.com:443/:b:/g/personal/seccles_cmrinsurance_com/EXDgzrrmhc1GnNui_DLzzBkBEUB0mDlJ3B08lrE-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://assets.onestore.ms	0%	URL Reputation	safe	
http://https://assets.onestore.ms	0%	URL Reputation	safe	
http://https://assets.onestore.ms	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://https://cmrinsure-my.sharepoint.com/_layouts/15/images/favicon.ico?rev=47BJ	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.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	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://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	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	
http://www.kkbox.com.tw/	0%	URL Reputation	safe	
http://www.kkbox.com.tw/	0%	URL Reputation	safe	
http://www.kkbox.com.tw/	0%	URL Reputation	safe	
http://search.goo.ne.jp/favicon.ico	0%	URL Reputation	safe	
http://search.goo.ne.jp/favicon.ico	0%	URL Reputation	safe	
http://search.goo.ne.jp/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/	0%	URL Reputation	safe	
http://www.etmall.com.tw/	0%	URL Reputation	safe	
http://www.etmall.com.tw/	0%	URL Reputation	safe	
http://https://img-prodsource.min	0%	Avira URL Cloud	safe	
http://www.amazon.co.uk/	0%	URL Reputation	safe	
http://www.amazon.co.uk/	0%	URL Reputation	safe	
http://www.amazon.co.uk/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/favicon.ico	0%	URL Reputation	safe	
http://www.asharqalawsat.com/favicon.ico	0%	URL Reputation	safe	
http://www.asharqalawsat.com/favicon.ico	0%	URL Reputation	safe	
http://https://cmrinsure-my.sharepoint.com/personal/seccles_cmrinsurance_com/_layouts/15/images/pdf.png	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms	0%	URL Reputation	safe	
http://https://mem.gfx.ms	0%	URL Reputation	safe	
http://https://mem.gfx.ms	0%	URL Reputation	safe	
http://search.ipop.co.kr/	0%	URL Reputation	safe	
http://search.ipop.co.kr/	0%	URL Reputation	safe	
http://search.ipop.co.kr/	0%	URL Reputation	safe	
http://www.auction.co.kr/auction.ico	0%	URL Reputation	safe	
http://www.auction.co.kr/auction.ico	0%	URL Reputation	safe	
http://www.auction.co.kr/auction.ico	0%	URL Reputation	safe	
http://https://account.micros	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
microsoftwindows.112.2o7.net	15.237.76.117	true	false		high
blob.bl6prdstr14a.store.core.windows.net	52.239.152.74	true	false		high
cs1227.wpc.alphacdn.net	192.229.221.185	true	false	• 0%, Virustotal, Browse	unknown
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
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
surfaceselfserviceoffertool.azurewebsites.net	unknown	unknown	false		unknown
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
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, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.dailymail.co.uk/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://assets.onestore.ms	RE4GG6p[1].htm0.10.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.asp.net/ajaxlibrary/CDN.ashx.	windows[1].htm.10.dr	false		high
http://www.fontbureau.com/designers	explorer.exe, 00000004.00000000.260104537.0000000008B46000.00000002.00000001.sdmp	false		high
http://fr.search.yahoo.com/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://in.search.yahoo.com/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000004.00000000.260104537.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://msk.afisha.ru/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.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.10.dr	false		high
http://www.ya.com/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.etmall.com.tw/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.hanafos.com/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.skype.com/en/	sale[1].htm.10.dr	false		high
http://cgi.search.biglobe.ne.jp/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000004.00000000.263518122.000000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://buscar.ozu.es/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.ask.com/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.google.it/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://https://cmrinsure-my.sharepoint.com/_layouts/15/images/favicon.ico?rev=47BJ	iexplore.exe, 00000001.00000002.449066469.0000014841BF7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.auction.co.kr/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.de/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://fontello.comiconsRegulariconsiconsVersion	icons[1].eot.10.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://sads.myspace.com/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://https://cmrinsure-my.sharepoint.com/_layouts/15/images/favicon.ico?rev=47	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.pchome.com.tw/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://uk.search.yahoo.com/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://https://www.xbox.com/20	iexplore.exe, 00000001.00000002.460756354.0000014846244000.00000004.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.gmarket.co.kr/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000004.00000000.260104537.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.google.si/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.soso.com/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://https://support.office.com/en-us/article/OneDrive-Help-5943c2b9-fafc-4cb4-95c0-9cc73fcabb30	sale[1].htm.10.dr	false		high
http://https://www.skype.com/de/	microsoft-365[1].htm.10.dr	false		high
http://busca.orange.es/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.twitter.com/	iexplore.exe, 00000001.00000003.402804838.00000148421A3000.00000004.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	iexplore.exe, 00000001.00000002.447661068.0000014841930000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263411384.00000000E1C0000.00000002.00000001.sdmp	false		high
http://www.target.com/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://https://www.xbox.com/&	iexplore.exe, 00000001.00000002.447510018.0000014841860000.00000004.00000001.sdmp	false		high
http://https://www.xbox.com/favicon.ico	iexplore.exe, 00000001.00000003.402095259.0000014842168000.00000004.00000001.sdmp	false		high
http://search.orange.co.uk/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://spoprod-a.akamaihd.net/files/fabric-cdn-prod_20201008.001/assets/item-types/	spoguestaccess-a0017cc2[1].js.2.dr	false		high
http://search.centrum.cz/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://service2.bfast.com/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ariadna.elmundo.es/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.news.com.au/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.cdiscount.com/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.tiscali.it/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://it.search.yahoo.com/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.ceneo.pl/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.servicios.clarin.com/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://search.daum.net/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://https://www.xbox.com/H	iexplore.exe, 00000001.00000003.401979890.00000148420C6000.00000004.00000001.sdmp	false		high
http://https://www.xbox.com/J	iexplore.exe, 00000001.00000003.402095259.000001484216800.00000004.00000001.sdmp	false		high
http://www.kkbox.com.tw/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://assets.adobedtm.com/5ef092d1efb5/4c272e8cc694/01c7c7ad42a0/RC278c787435b94d148603e89a80d2b33	RC278c787435b94d148603e89a80d2b336-source.min[1].js.10.dr, launch-EN7506e353034849faa4a18bc4c20e727c.min[1].js.10.dr	false		high
http://search.goo.ne.jp/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.msn.com/results.aspx?q=	explorer.exe, 00000004.00000000.263518122.000000000E2B3000.00000002.00000001.sdmp	false		high
http://list.taobao.com/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.nytimes.com/	iexplore.exe, 00000001.00000003.402804838.00000148421A3000.00000004.00000001.sdmp	false		high
http://www.taobao.com/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.etmall.com.tw/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ie.search.yahoo.com/os?command=	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.cnet.com/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.linternaute.com/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://https://img-prodsource.min	iexplore.exe, 00000001.00000003.402214192.0000014846225000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.amazon.co.uk/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.cdiscount.com/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.asharqalawsat.com/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.fr/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://https://cmrinsure-my.sharepoint.com/personal/seccles_cmrinsurance_com/_layouts/15/images/pdf.png	EXDgzrrmhc1GnNui_DLzzBkBEUB0mDlJ3B08lrE-XQmbmg[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://search.gismeteo.ru/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.rtl.de/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://https://mem.gfx.ms	RE4GG6p[1].htm0.10.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://spoprod-a.akamaihd.net/files/odsp-common-library-prod_2019-02-15_20190219.002/require.js	EXDgzrrmhc1GnNui_DLzzBkBEUB0mDlJ3B08lrE-XQmbmg[1].htm.2.dr	false		high
http://www.soso.com/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high
http://www.univision.com/favicon.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.00000000E2B3000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.ipop.co.kr/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.000000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.auction.co.kr/auction.ico	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.000000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.orange.fr/	iexplore.exe, 00000001.00000002.448613692.0000014841A23000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.263518122.000000000E2B3000.00000002.00000001.sdmp	false		high
http://https://account.micros	{30158FA8-5616-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://onedrive.live.com/about/en-us/	sale[1].htm.10.dr	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:	339264
Start date:	13.01.2021
Start time:	19:10:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://cmrinsure-my.sharepoint.com:443/:b:/g/personal/seccles_cmrinsurance_com/EXDgzrrmhc1GnNui_DLzzBkBEUB0mDlJ3B08lrE-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:	26
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@6/346@21/5
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, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 88.221.62.148, 2.20.142.202, 2.20.143.23, 92.122.213.248, 92.122.213.216, 51.11.168.160, 23.210.248.85, 152.199.19.161, 23.54.112.217, 152.199.19.160, 92.122.213.240, 92.122.213.194, 23.210.249.93, 84.53.167.109, 92.122.213.247, 23.201.255.153, 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, 92.122.213.219, 92.122.213.200, 92.122.213.176, 92.122.213.193, 2.17.185.83, 13.107.246.13, 23.50.99.143, 205.185.216.10,

205.185.216.42, 51.103.5.186, 65.55.44.109, 92.122.213.163, 92.122.213.195, 23.205.179.153, 23.210.248.45, 13.66.138.97, 20.54.26.129, 51.104.144.132

- Excluded domains from analysis (whitelisted): assets.onestore.ms.edgekey.net, cn-assets.adobedtm.com.edgekey.net, i.s-microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, wns.notify.windows.com.akadns.net, www.tm.a.prd.aadg.trafficmanager.net, a1945.g2.akamai.net, star-azurefd-prod.trafficmanager.net, statics-marketingsites-eus-ms-com.akamaized.net, au-bg-shim.trafficmanager.net, account.microsoft.com.edgekey.net, global.vortex.data.trafficmanager.net, ris-prod.trafficmanager.net, compass-ssl.microsoft.com, lgincdnvzeuno.ec.azureedge.net, assets.onestore.ms.akadns.net, statics.onestore.ms.edgekey.net, c-s.cms.ms.akadns.net, ris.api.iris.microsoft.com, lgincdn.trafficmanager.net, cdn.account.microsoft.com.akadns.net, a1531.g2.akamai.net, spoprod-a.akamaihd.net.edgesuite.net, c.s-microsoft.com-c.edgekey.net, compass-ssl.microsoft.com.edgekey.net, cs9.wpc.v0cdn.net, a1985.g2.akamai.net, e9412.b.akamaiedge.net, compass-ssl.microsoft.com.nsatc.net, i.s-microsoft.com, statica.akamai.odsp.cdn.office.net, iecvlist.microsoft.com, par02p.wns.notify.windows.com.akadns.net, go.microsoft.com, prod-video-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, 160c1.wpc.azureedge.net, ie9comview.vo.msecnd.net, cs22.wpc.v0cdn.net, mem.gfx.ms.edgekey.net, cds.d2s7q6s2.hwcdn.net, login.msa.msidentity.com, c.s-microsoft.com, e7808.dscg.akamaiedge.net, waws-prod-mwh-031.cloudapp.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, mwf-service.akamaized.net, arc.msn.com.nsatc.net, e13678.dscb.akamaiedge.net, e11290.dspg.akamaiedge.net, www.microsoft.com-c-3.edgekey.net, query.prod.cms.rt.microsoft.com.edgekey.net, login.live.com, 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-marketingsites-wcus-ms-com.akamaized.net, web.vortex.data.trafficmanager.net, e10583.g.akamaiedge.net, t-0003.t-msedge.net, e55.dspb.akamaiedge.net, dub2.current.a.prd.aadg.trafficmanager.net, blobcollector.events.data.trafficmanager.net, privacy.microsoft.com.edgekey.net, www.tm.lg.prod.aadmsa.trafficmanager.net, e2699.dspg.akamaiedge.net, account.microsoft.com, 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, emea1.notify.windows.com.akadns.net, img-prod-cms-rt-microsoft-com.akamaized.net, client.wns.windows.com, statica.akamai.odsp.cdn.office.net-c.edgesuite.net.globalredir.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, Edge-Prod-FRAr3.ctrl.t-0003.t-msedge.net, web.vortex.data.microsoft.com, lgincdnvzeuno.azureedge.net, privacy.microsoft.com, e13678.dscg.akamaiedge.net, skypedataprdcolwus16.cloudapp.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
19:11:13	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\KLUDLQH9\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):	133
Entropy (8bit):	4.6866444638864255
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsnObemKmlULF0VqHlJR3DcRlLRJAqSRCHNaKb:JFK1rUFjgemKm6GVqHlJR3ARlLRiUHZb
MD5:	FF8F98779ED4906B132207B569868EEE
SHA1:	BFB926042F562DB674ABD2EF82A1FAD4ECC05D43
SHA-256:	280405822338421B9BC2EF9B3B6E2AE702FE0B402B1CE562441794D7F4AD543C
SHA-512:	5A7386719D296624482FB59F6A9549BBF54AAA4DABE02A1E8217B635D6FB7F2F4854D70E2783DD85A658486404D4DE433BD04D847331B9F30781B7CCEF8F8F0A
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="com.adobe.reactor.dataElementCookiesMigrated" value="true" ltime="97986736" htime="30861859" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{1D8FBBF5-5616-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	60616
Entropy (8bit):	2.1301040434169396
Encrypted:	false
SSDEEP:	192:rWZVZx2Y9Wxt6fcFMfeufy8r+QmWdqhwHW8DVQWW:rSbAYUDYBfekz+ldq228B+
MD5:	ECE9476D9122D280976483458BC45C60
SHA1:	E1201E896331AB0C81C387556C304EAC18D70261
SHA-256:	D378C24168ECDBA995456ACE0AD3DFEB2AD709E1B56BC47C477E94CC884F60E9
SHA-512:	22998570C4ABE01307DA58AF1F3083442E8B0A8F8CB28080DE9CC7D5EF9C22D1A070D73CBE1568B84E808379B80E6E5F00A991BF8FDE9F7B877292C85847716A
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\{1D8FBBF7-5616-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30730
Entropy (8bit):	2.2972651588428605
Encrypted:	false
SSDEEP:	192:rfZQQd6PkRFjd2TkW/MGYTk9MYPxOqGjHZNrKjhc58fspA:rBpIMRhU30GWk+YPxOqGlNrKm58US
MD5:	FB31EED5C8EA570B1DA6A2A265AF1420
SHA1:	8E1640C50E1BFA9D205B5E753AE46C016ED6DB7E
SHA-256:	F745481F07EEF75FBBD6E539D4FBFFF26DF572DB2E072E9D34E1914B01BB41D2
SHA-512:	9C40B99A293131551E5939B22A692B872C2EF46247453E6C9C1B403FBDFAC91271AD5E057F32562D149671840947D817A230C19CB3464540456F88F2555AE185
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\{1D8FBBF8-5616-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5853648648393635
Encrypted:	false
SSDEEP:	48:Iw7hGcprsGwpaThG4pQ1GrapbSExrGQpKdG7HpR8sTGIpX2pUGApm:r7ZEQv6lBSIFA8T84F5g
MD5:	15EC109FB6FE9B95F7AF251CC948490D
SHA1:	5A45C241571ED847D1432BA0C5688428FDDA9ED3
SHA-256:	9E5FD58E1DCD1A6C939B9E9E63EF19FC547E9421CD5A0FF257D2E858F2C17424
SHA-512:	89ECD28AFA7FA851E0CE9540F25C727FCBE33B4C79F828FF6E4F6B4E5D5AC7871B28ED54BA84ECCF5B9748D761D140CB4A22E20A535D25EEC6D013CA0AE0EB1A
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\{30158FA8-5616-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	205748
Entropy (8bit):	2.584114309163759
Encrypted:	false
SSDEEP:	3072:Cj/gDx595pv9aelklvpRnk/sDRnk/lv+lseQ:UQ

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{30158FA8-5616-11EB-90E4-ECF4BB862DED}.dat	
MD5:	691893C86832AD73BAFD7B9806FD7B26
SHA1:	BDC7803822235AAFC3D374AA54807B67D8A14444
SHA-256:	AB2FE2825DBC3CD74190179F96A74FB4CFC8C08792EE6A9BC256D557D44088FF
SHA-512:	6C6639E3BDB9B13EBEB6D495B0349B0C11E71A63B9D024ED35BF46659B0F25594A28541C9E8CED437D24B7E58A3CDAD5864F4986D7DCB80C71D726D949BC8 13
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\{39540F1B-5616-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5669289253039123
Encrypted:	false
SSDEEP:	48:IwnGcprqGwpa0G4pQsGrapbS/rGQpKXG7HpRWsTGIpG:rNZyQE6qBS/FA2TW4A
MD5:	E299C17E63D905CDA6457FEA6097B086
SHA1:	2C475B3B4F15236443B03F8CB8CB63B4B0F47E2A
SHA-256:	509C938AE3BD7F6C8998C8BB4C02FBAC1A363A61F8D5BF1BA6C44B79486237DD
SHA-512:	0FE2364E2BFADFB3C4BFE8963015DF002A7F536F8129C5F4CFC93961439A8DEE4523EFFBAEA9A0118F35314D6C21848C3A92042844FCCC3FA8B4DC149D974A2 2
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):	5.07243362690565
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE2OZqCnWimI002EtM3MHdNMNxOE2OZqCnWimI00ObVbkEtMb:2d6NxObQJSZHKd6NxObQJSZ76b
MD5:	55C37E382A3A6C79574DE122F8E8C1DB
SHA1:	B095496CE6246C55BDBCBEA3451CA51EAD86BC15
SHA-256:	42EEEA1BD2F739D022456B25A2942E740BD79DB4FC16D7C4A7240C86571F8EBC
SHA-512:	1242107A8DBD64BB8148CBED98378F7D9F3C076FB1631826AFB3B5BB8AD96E3067B6483CE1C83182B7DFB75CAF33240EFE888C89CC308EE0D0082CC2076829F 3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xf40a3f11,0x01d6ea22</date><accdate>0x f40a3f11,0x01d6ea22</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml ver sion="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xf40a3f11,0x01d6ea22</date><accdate>0xf40a3f11, 0x01d6ea22</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msappli cation></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):	5.109771236367875
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2k+6J2CnWimI002EtM3MHdNMNxe2k+6J2CnWimI00Obkak6EtMb:2d6NxrASZHKd6NxrASZ7Aa7b
MD5:	03E3A1232846C3397034CDA5861936CC
SHA1:	75B2ABD9D993890019CF6369BC72B6EF58E69BE9
SHA-256:	3118AA2A95958EB9B15D08BECDAF06EFAA72B7DB9BDCDC6EBBD129E1E8F5FF8D
SHA-512:	543DCAD278CCC12580ED8236E613BE650D6F1464FC09C4D8890A091653E7B7C775E20735F6CD247BD03EA3972C0BDBB6275C31498890F7339CCDDBD38986DE
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xf3f98ea2,0x01d6ea22</date><accdate>0xf3f98ea2,0x01d6ea22</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>0xf3f98ea2,0x01d6ea22</date><accdate>0xf3f98ea2,0x01d6ea22</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):	5.082878217005761
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLKoOLoqCnWimI002EtM3MHdNMNxvLKoOLoqCnWimI00ObmZEtMb:2d6NxvnVJSZHKd6NxvnVJSZ7mb
MD5:	46AA21F65A675EA351CAC1158DDB2D47
SHA1:	7FE2612C5888EFE160966598AE86906A2D6E9D05
SHA-256:	2D3D230EB92A8EC85BF523F7BB4B8BFD05720CE1D10BFCC82197E41BB3F79D0D
SHA-512:	8F985F28813D33F43B1D5010D7FCCA61EFBA0BFB2A9D7AD21E507C36D3AA8D105BF3EDC653EF567BA5A7800896C2531A9367EF6958A2D642800AC751736254F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xf40ca17a,0x01d6ea22</date><accdate>0xf40ca17a,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>0xf40ca17a,0x01d6ea22</date><accdate>0xf40ca17a,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):	5.105528782789595
Encrypted:	false
SSDEEP:	12:TMHdNMNxiGD9dCnWimI002EtM3MHdNMNxiGDlCnWimI00Obd5EtMb:2d6NxYSZHKd6NxySZ7Jjb
MD5:	75BD1295F8C18F0D5D6088FB62F16DDC
SHA1:	7E1A89B5F60073B4A3CB929F754DE3B2F96D56EC
SHA-256:	2B25ED59E7C1DAE2DCFFC3D9AFA8FCFFE5F5066604AF8A4EB8FC2FDC344D6C8D
SHA-512:	695D770589CC8D68EC86A4E911E9F9198832DE3595EFCE1BE0B9576B55D8E166C8EBC293107A2E830D8D6540EA91D609246E673F5A8044F09D9BE72236154742
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xf403180c,0x01d6ea22</date><accdate>0xf403180c,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>0xf403180c,0x01d6ea22</date><accdate>0xf4057a71,0x01d6ea22</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
Size (bytes):	656
Entropy (8bit):	5.106739584175763
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwFOCqCnWimI002EtM3MHdNMNxhGwFOCqCnWimI00Ob8K075EtMb:2d6NxQ4XJSZHKd6NxQ4XJSZ7YKajb
MD5:	A0D8A777CEB5A7AC1E6E5132CDB6D254
SHA1:	72C4A34D62879992C9D7323838C3854389211F83
SHA-256:	B58A1EA7277FFDCC6BF55A0789164104DABBF0E28FDCBA1B41266BAB988DE3A6
SHA-512:	ABE847C2239ED6D8EA77F09880141AFC83883A107AB2A35214CF4E1E29BC34FF1994F7A90C544E29EBEFBE1742BD101DCFD746106E17BC625FE12979B4EBBBE1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xf40f03c3,0x01d6ea22</date><accdate>0xf40f03c3,0x01d6ea22</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>0xf40f03c3,0x01d6ea22</date><accdate>0xf40f03c3,0x01d6ea22</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):	5.080225283787341
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nEjCnWimI002EtM3MHdNMNx0nEjCnWimI00ObxEtMb:2d6Nx0zSZHKd6Nx0zSZ7nb
MD5:	0981E7D32EE612D1EE0E6E28A34AA57C
SHA1:	5D001E814727F8F1786CBA08C24D43784D21545D
SHA-256:	617EEBDF1FE97765964097FF56CFA455280D4F7E2FF0078952AAEA1BBECCCC88
SHA-512:	CC494F925E50379FC4FAE3F53D029D3AC0A8635EFB3CBEB3D847256487E1E2DE9CA27774EDBA70AA973235F6196E252D837AE43BC06A41DADDCB1E316F9CF9C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xf407dcba,0x01d6ea22</date><accdate>0xf407dcba,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>0xf407dcba,0x01d6ea22</date><accdate>0xf407dcba,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):	5.134711429299707
Encrypted:	false
SSDEEP:	12:TMHdNMNxxSlCnWimI002EtM3MHdNMNxxSlCnWimI00Ob6Kq5EtMb:2d6NxRSZHKd6NxRSZ7ob
MD5:	E82ECF6671F73952C240858631B2DEB7
SHA1:	BE52954C8BFD0FA35D294EB33E904C67CF269D6B
SHA-256:	17D2C80E7F3F7D368CF238B8C03CCB0F34CD0CA7C4A799C8040EF2B1A37F02CF
SHA-512:	3A024DD252990C03AD33A4FF2726522C1DF7532FFE020CE06B69FD9F7EB0E0EEA4A0DDBE5E114307D66E1CBDCB941AE4D4712AC262BF5474B790632AB480407
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xf4057a71,0x01d6ea22</date><accdate>0xf4057a71,0x01d6ea22</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>0xf4057a71,0x01d6ea22</date><accdate>0xf4057a71,0x01d6ea22</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):	5.100974221433746
Encrypted:	false
SSDEEP:	12:TMHdNMNxcy6x2CnWimI002EtM3MHdNMNxcy6x2CnWimI00ObVEtMb:2d6NxrY9SZHKd6NxrY9SZ7Db
MD5:	861AA60CE6E585A0D17753D8A28F0A01
SHA1:	A7841726153CEFA42EDF4828A8FB8F9E99995F77
SHA-256:	1E7051D1657313A69DF6BDDA6F35CC388279F7DD5B57BC619DFB4F6B86D478E8
SHA-512:	CFED4AF6D862F4EE4D8D225E34AAE8AFCD47F89AFEADA5AC926D3B16AB1F01D6D6E3EDFE7360C909BC9046D4F4B30722C8BD145E15D96146B761C85B65F86B18
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xf400b5ba,0x01d6ea22</date><accdate>0xf400b5ba,0x01d6ea22</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xf400b5ba,0x01d6ea22</date><accdate>0xf400b5ba,0x01d6ea22</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.083912038631469
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnGD9dCnWimI002EtM3MHdNMNxfnGD9dCnWimI00Obe5EtMb:2d6NxbSZHKd6NxbSZ7ijb
MD5:	486F577ECB31FA8EBB5D3BF151741150
SHA1:	41FFA8E923AC4B962AF01A4A12D38F4171C5B71B
SHA-256:	4E5D219F86DA98AB59FAA9BB7297DF95A6B13C87F61FC0ED033D2A884C0BE084
SHA-512:	4B734FF716DB3AA4F28B537A2D4D3BD5FDE3CAC4CE8BE7E65CA606DAA6F357B5D37E1EE5325F67BF500B8CA720D2BAE9EA02FC0FB72BEC86162089FDE9789 5DF
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xf403180c,0x01d6ea22</date><accdate>0xf403180c,0x01d6ea22</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xf403180c,0x01d6ea22</date><accdate>0xf403180c,0x01d6ea22</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	53748
Entropy (8bit):	3.039730217908053
Encrypted:	false
SSDEEP:	48:bAJAgAgAGgyyyyyyyyyyyyyyiA0/A9QQQQQE6Kk6pk6xk6tgyyyyyyyyyyyyyymk65:eQQQQQ65h6ZWQQQQQb6D7wDmQQQQQFn
MD5:	9774DDA1C81FF7EC6C8E9F8D8539ED5E
SHA1:	206CD9B6D5D67BB2EA87CC4974B0DA80A57ABE7B
SHA-256:	C8EA76BD4FE1F7EE783C63218AA0152498010669ABB57725E6C74913E90120C0
SHA-512:	B993EBC2D004E85132D355D479347CF1E71815DFFFCE36D7292240BAF4EC8ACD6BC6662E28545231FD39AFEF0821862A2754CB20D602D83C0E71111DD7BBE09
Malicious:	false
Reputation:	low
Preview:	(.h.t.t.p.s.:././.w.w.w...m.i.c.r.o.s.o.f.t...c.o.m./.f.a.v.i.c.o.n...i.c.o.?.v.2.~(................h(......(....................(.....................................''P..'' ...33333333333333333333333333333'' ...33333333333333333333333333333'' ...3333333333333333 3333333333333'' ...33333333333333333333333333333'' ...33333333333333333333333333333'' ...33333333333333333333333333333'' ...33333333333333333333333333333'' ...33333333333333333333333333 333'' ...33333333333333333333333333333'' ...33333333333333333333333333333'' ...33333 333333333333333333333333'' ...33333333333333333333333333333''''''''''''''''''''''''''''''''''

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1083_Panel13_2Up_Pro[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 494x278, frames 3
Category:	downloaded
Size (bytes):	38605
Entropy (8bit):	7.98190244701047
Encrypted:	false
SSDEEP:	768:dxMQ8yVWBoP3XhtdmOhA8eYxRnB0UQ1XuTIvdQY3xRo9:rMQnVWBWXVm8U5CW2Y3m
MD5:	D9809D83657B6EB4E6C7C57DC49C58A9
SHA1:	12F9742B37C01AFF73CC0D0365AF695EA2391E03
SHA-256:	F9EA18D47A069C318175C5914520227B36FD3A1DA7857DAE94CBE3008C19F99C
SHA-512:	E401C5F3B8E7066C63583BD4BFED912ABAC43862BC0B3FCA56755B3E0C9683A750885166331DBAA4C72BF39B757D28A682A9A595E8970CD6B1C607C9D222FA 5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1083_Panel13_2Up_Pro.jpg?version=846c282c-e61b-1660-6231-f045de3efdb4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1083_Panel13_2Up_Pro[1].jpg	
Preview:	.....JFIF.....!#...SSnW...h*v...kT;8<;.. 4g>2.Zik.e..B.....x.Z..=.%Q_....`.*.t.q$$..O.....z..}.....ZT...Z.E.:W2o9I...3....P..Y=.3.!V..p.i....*..P!l=a.<...W..<..<..P...`..';.c.Xc.B..q..d..4...)j...e....]V.&...7.89>...{dT.(.uJl....W a..c.yU..,..-X....T.4Y._:vV...hFa..JH..dw.V....ou.....2..r...os.c]..f..0.4..$..T/<..<...N.C.dF.!e.-m.b|V7.....r..Y{Ro.....eh.g:..F...%..(.!.NR.=.vU.w..-...(.KNf..3.74.\{".F....kX...Q..q.q.. ..7._BE6F_F..h.+.y..Y.nn.".).rKl..F.....@..K."....v..6`.].3.w..HS?=...:C.....#.....v...l.d6.Qp.0.O"....@\.....:.M.t...MXsp.....=.c%.....R.MM....Zl..C.m...5A...).~.....,..%.S....)...{^"d .T/.:.R..[.z..g.."#4.e..._.....7K%.s`..Z+A...TC...ai..p.=.....S.....-.w&...x@E...^.^_...<..P..H.fN.w\].7..%.....t..}..Vr..I....O..GV...L.N..(lw.~..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1083_Panel13_2Up_home[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 494x278, frames 3
Category:	downloaded
Size (bytes):	49954
Entropy (8bit):	7.984603554530586
Encrypted:	false
SSDEEP:	1536:yq3anxyX0NSIlzwOxGxwTuzw/YMiGJ80ESD:mYHINwOxGxtzMYhGu0ESD
MD5:	6F473E942CFC0F770C2CE6D22B92D6C5
SHA1:	93D9DD1A2D88374477CC18F5A70AAF3CC1F7B086
SHA-256:	07FF3D2FCBB0F7DF9CBAD5FEDC5886BD103CC881CEFF479BF7DE39CF8D31E91A
SHA-512:	FE2976A2789E921A61DA800521A5FF301CC9B27110C0AC1A92EF39A89685AA157CFA336ABEDE10D7EDDB5C0EBF82919407346387670A643AA3E6B0DCD7D219 4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1083_Panel13_2Up_home.jpg?version=402e3849-72f8-ce84-c458-e4237dac71aa
Preview:	.....JFIF.....=ff.b..<..@x.\..7....35....["0./b .t_....l[.....{5.lb..y...o5...9...P4..m...9l.G...7....^Y..o.uO..#...333[..k4....kU....($..-.Y.....-.o../Nz..3y...4.kX.. ....y.R..u,....f....?.$k.?GX..=ul...fo33...k[.@.o..iP..%.NW3T.|.k33 y..=.....p.L.o37....0:.:{.%..q.hu...;..s...S.L.....g<u.....[..oY...h9.kX.ai..v\1...;j.....|...7aR...&O;....*.,...F`.7qf`.Z.#]..Nf....e.c....U.....n.....I.K:k../.....N..c'W.....y.y..WBt..`H... (.>...}rX..T...9<.....e.S..y..{..*.lP....?..w.9.l kW.)k...z&G...!...,).....oIU...{..x^.._.nfb3.>E<.M.l!.....Pf..;..D....Mo...;&..=~.?y....X.K."..../..0..pv.....gqd..63N..VE.../...bs..\."..Gki.... .....OH...u.2u.g:..\D..E.i....b.kJ7.....*.rW:.5...N.4..>...-...g.b3J..Y..6."f-.....g*X.9...-...H5..W=^.>6._MMN

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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:BIvLs1yU28KxNBdFs/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....$O.u..N....or.w.z.Q#..2..UUJv.....(.3;.....*A."""""F...9|...O..6...U%'..0..y.%.`...Y.F...kb.G.....E.b]..".....mk%O...H.T....2.-...q..@A.PPS..i.m]... (A.`."".~.i..=L.H.V.=..l.....eq`..T.@...\J..$..0.%.x....222".....|.YX.G.@....g.0^x(...,6.Y..URRi%V.....-.sQ..\..i.....x.x...F..J.UH..X...E8.3p....3.Z. ..Dps.M5..`.=.....H.....)..\p.q..6:K.1Iy{....G...`.m.m.6.]...d...l..c...V.OEx.....oK.%U..G....s.1Nj..m.i...]o1. ..W..K|.Rf..b.3Ey.....<...//Y..A.I<...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..Fjjn..F3#p.q..q-...n.cz]..?..m.(<..c.'M...;.q..=#....c.SCkf ...q.*.n..:.<....m

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1083_Panel15_Mosaic_Item5_Stand[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 542x400, frames 3
Category:	downloaded
Size (bytes):	16475
Entropy (8bit):	7.814365220066478
Encrypted:	false
SSDEEP:	384:fbZaAb0yUMZ95IQRVAfobZCXLd/ZIFNHNY9tFiINeFwsQqH9:DZgySQjBShANa9tFiINe+sQw
MD5:	A2AA2B4620EC4C797042811C008D3B89
SHA1:	B23CE846CC395867F219C33C42A094197816B9A6
SHA-256:	FBCE541750335AE8C5BB4839F2D7EBCFC7B5224E0CE01B97C17EE89E6ACBBC80
SHA-512:	34B8032574C430C5639BAB431DA8BDEAD67819666728173787D4BBD3DFE6C9A48EE6F21172EDAC5D0C7B46455BE6954A82E9BFC996126922DC2854129D3741D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1083_Panel15_Mosaic_Item5_Stand.jpg?version=00530597-9619-2575-35f4-6d87092a5ab8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1083_Panel15_Mosaic_Item5_Stand[1].jpg	
Preview:	.....JFIF.....!.GS:-.zi.Q...vi....T.EB*.E[..|7 ....a..@...+.H.V.+.....AC.f....PT..aR.-.W...@..1~h.....U...3.=.nN...c.....".XT.po$6..zO.!.+..8.....`(T...rO_y.T."...3....QR*.TB+....]...".R...8...X"..V.*..g...*EJ1.f...V.H.EJ..w....=.. .T.8.Y.....*V<..?w.;.T."....T*V.*U..._....8T....?.@..V.H.+....._>..V..X.2...X....D".l.k..k.AR*....2...."..(T...=..z.....1.c...."..+..W.....v@*V..F:.@..T"..".Q].....i..Ua.1.b..V. ..*T.t....l. ".TT.c....X..*.a...*..Q.:..T.Pc<...T..T..!.t..<{.,.D".aP1.f....DT..TU.<..G..U.+..W...."..".V...A...^.n...U...?.....B..a...9..j.n..]..XEQ..8.G."".....a.V..o].g..S./au.!.D.*p....."...W.y...#. .R7>...../.....EH.T..L!.=UU....U...p.....!.+.7.....Tu.{..U.....9t.....a....v+...~t.3T@..X.Yt....EH....t./w.;,".P..a..T+...D@"...T.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_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, 474x535, frames 3
Category:	downloaded
Size (bytes):	38865
Entropy (8bit):	7.980078611234522
Encrypted:	false
SSDEEP:	768:mEGL7hkkmRKCcuJzZVHlxylKKVnd7MlzYuJRwM6gXoXyKDUuoXxV:kxktRK67Dxyl6ukQYCKDUL
MD5:	EA6CFD35139F324A25283AA826F64817
SHA1:	F967C6A816D0E8FCAE96242890ED063E28CB85AF
SHA-256:	58E3919BE3E7A001F10FD8C1E16DBB40EE3CC48F91A2858D0A97CFA97A3D327C
SHA-512:	22CB909EE15DBCE0429E7A3FEF464DABFE6EB82EB764619CE370A021D7B320B8C631CFA0A205A6F646E2890B35EAB406EC64A66BAA506566FE2B60B83B519E 02
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel01_XMosaic_DoubleR_Alfred.jpg?version=4894d85f-5cc3-e99e-e112-8d7eaa70fbc7
Preview:	.....JFIF.....KI2d..2...a.....(i...|b"1.b).>...I.I..... .....1.F8...t9...3....u.&I.<...00.....F#.P...1.....E...I&L.t,..X@D..1..O.R.. L....]BI2L.2B.^(...@F0.....30.$F.QYn.$.3".33..\Y.@@@..8.S.U.....q.4.d.t....D@.1.....OCY.a.,.a..... $).L(Y.,"... !.E.>....&.)..;.y$.!E2.L/.qa.....(.u}.b..;'"..4V.I&fE2.L/.q.....*}_@..3.19G.%..I..L....Y..@D..#..W...vwd....Qj$.d..8..x+.0....F..p.....$Q.e..RI2fy.Y.<..X.@..8.0..}o@...$. <\|.l5..L.<.R.x+.....@!.P..z..:H...-.q$.3'..B..a...h."...].+ I...}.i$.3'..B.^....4c.F...4...d.$..q.I$...fHE."...1.4q..N..$).$. ..u.I$...fHE..``.....c.8i....,.$.$...$..y...P..a..B1..0...gL...[..)'v.e. ..I32y.&aQT.`.....8:<o..s...=.....I.+tn.I32yY&aP..`...`.@.....f....{..L...I&B...3.....F.. .....?5Ks.....K..@.$...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_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, 474x535, frames 3
Category:	downloaded
Size (bytes):	63300
Entropy (8bit):	7.987195829720056
Encrypted:	false
SSDEEP:	768:L2DRvSPCm+jRQnelT1EJYsexQ/7Vu6RQH/vT22Cs42kD/4ZiaS:L2DRFpanih8sMR+vqW42kD/Si3
MD5:	0EB5CF733964E5680B0227C962E89465
SHA1:	B9D5BADDFEF724B2D6EA533F41A7A7413FDADC75
SHA-256:	64551458148E4202A50FE7F5AF3A9A9D1F8663E2F9DCFCC6296BA2EDC1F6EEED
SHA-512:	979DA68F306DB204F54C1909223733BACE51AA1654693EA42E3BF098F815E7D21F9A378AC5FE9A524DB23AEECE760F88016B138D5E1B0C9964135C1381B335CF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel01_XMosaic_DoubleR_Jen.jpg?version=e7f17bdc-c71a-0138-a354-b9d551c4eb56
Preview:	.....JFIF.....B.~W{.|.s...s.}.>...6.!.!)....<.P.. .x.]...g.u].9.y.s..>...>.....BR.%.i.w..[...4.w....9.....m...i.8..)O..M..6..[...5../.&\...O..y..P.Km..m.<JR...Cm2...9..G.~.....G..YD'.&H..9.(T...m..<O.....c..:....&.}.:.....D..m.a...b <D...P.[m.!(.?..O.....$.Ml.....h5V".D8..63q...F. ...i.i.%(.D1..'.C.u.....\..B..b,X..L.....8o.^...6.....)J9.s.'.)...!.9..}...<X.....e..a.*.....!.q.Bx.'...j.Z.l..c;z....U~..0..>.v#..@.Nj.a0..L.R..<... {.>...u"v.2.....I.H.....0,d.0.. _~N..B...V.WAV.H X.R...F..u}...[\.{l69....!....Bq.3a.)q../..4jo.C.eN.=Mo.88@.EB....nu:...]j..y.6.....T....)lEC....j.\[...Q..h.n.6..R.....1.Sb.+...-..3.6=l.....m !.....u. ....O...m%...A<..0..9..t.....2.#...".Ur.u...M...8.....!..J;U.fn.....e.X.....V.v-....{,..J.jD.....$..H...$.X...'

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_Panel03_Banner_Resources_Homepage[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 319x175, frames 3
Category:	downloaded
Size (bytes):	28299
Entropy (8bit):	7.976604396821143
Encrypted:	false
SSDEEP:	384:fyd1/E4+NGYvfFy4f0G4kVm04ja1udXGXE5mlAbJbure0G+l8PQ70w6+J+EEHt+8:9zFhcG4YX4jzQU5m5qr8z1w6+IEl+ir
MD5:	81B81DF29C589AE634EF9F1731EED78E
SHA1:	171FDE917AB8CC47A5A95DCB2DCF8528E2D46519
SHA-256:	BFD49026E2D893819A4FF255D9608ACE99D9D6258CAF180D66ED8542234627A1
SHA-512:	36DFBF39B6E4F4059918F21939AED76F2739AA1398B6F228A033932D4F532A38D546B0F7374FB4F7DECC74332B333A2EEBFD2BA48366D7941FCF1D4F132A41A7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel03_Banner_Resources_Homepage.jpg?version=6bdd3f9b-b070-2398-fa99-5ee3712626a2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_Panel03_Banner_Resources_Homepage[1].jpg	
Preview:	.....JFIF.....?.....~...).`G.#&..[.TW.p.|.Q.xA.dZ.u..'.P<.%.n.f,..W..S.....&.r.f..O..V.6..T.^.}W.....j>e.e|O.8A....l.:s.. ...C....w....U..B.6.....7*h._".E...;h...Z..M.\{..;.l0<....u. .H..D}.T.u9.h.S.....nl.{..Fn.0;...=|.....1-',.TB..A.^...-...f.Q..$..S."...U.fr.5..%f...gJ(O]K.....n..DcC.?.p...z.6.....W.H..".....'.Y..j.$~.>|_.+x.U...&J;.2.Q..vD...s..lk.6.~.. .$".i.3j.....3=[..`A8..D.5.V.....!.**.".....q....{e..J..Z.\.....E...<...T.Q...F.1.}.].J...+...L....;.j.'.....(..>b.Vp.....fZ.!..5.^.T..@.w..zV.....~M.qY.}*#.xV.\|..9.....6.v..(mA...y..m@.[..M.^..._4.utrF..4..q..UT.5J.....~~.y...5..v..(.>O[.%....v.....ZG^..(.$..:...^.,.Vz..IR.....8S..ck..`;Nm..#s.d.Z.Am.ay.....Z...;.P...auZ..T.W)4...H.6D.....\<..G.TM...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_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, 1040x585, frames 3
Category:	downloaded
Size (bytes):	203429
Entropy (8bit):	7.98185656353096
Encrypted:	false
SSDEEP:	6144:bxoyLwTeg3no8fygJ0A+jYBxFTpz9exiQDV8:b+uwB3nXfyO/B7Tpz8rV8
MD5:	854C404B59E82CB04424E09A12D09BF6
SHA1:	764993A09A1D105BC1AB0D3894170A1A7501BC55
SHA-256:	12ED0D8889E4CE988ABC29B6E251A791C389CF56BFED6A6BFFD1B72C19C15DC2
SHA-512:	BC37D4644C91E51724D06872FD2EF6CDCACF92FCDA91CED99D0F8472DB58EBC2847B14072822D37BAAEE0126D921A60046A3220C20273397BE42CE894DD2E4B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel04_FeatureGroup_Need.jpg?version=0403d7c9-4711-8f9a-cb4d-38274bf57476
Preview:	.....Exif..II*.....Ducky.....J.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:E9A523555CD811EA88EEDBD181122FD0" xmpMM:InstanceID="xmp.iid:E9A523545CD811EA88EEDBD181122FD0" xmp:CreatorTool="Adobe Photoshop 2020 Macintosh"> <xmpMM:DerivedFrom stRef:instanceID="38C3F81A8565C710B5E916AC02E087A6" stRef:documentID="38C3F81A8565C710B5E916AC02E087A6"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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:sELN5aV7sH8XYyNwEu6ut37dGM1lSdi+17lZKAGTaeyUSmN: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.....l.....&%C.s\L.....e..7..&..P.Cg...ms.#DHU...G.*....""*.d..Q..H.I..}.....}....+e.:.A..L..R.....5...}K..~.b.V..tz,...+y.z]...m)4.M]1.H..Q.....6#..H.D$r5.9.s.{....G.M..#..[.....nN~.3[..6Y.&H.(c..1..._.....7B.....b.....Dt<h...Y$rF..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.}Bl6d..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\INetCache\IE\0W10PBUV\1920_Panel24_3Up_Footer_Surface[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 485x273, frames 3
Category:	downloaded
Size (bytes):	35907
Entropy (8bit):	7.983363992036313
Encrypted:	false
SSDEEP:	768:KmVByvtbA1x6PV9SY+/l7uLx/1YymkGrFXlJ45vGr9c2YhlyYnT:/VkyOPVU8kDYymZXlJ45uK2YhQYT
MD5:	10CB709B4E0906D84228CE55C7CC74BD
SHA1:	7C015A6D1D5058B82BFFAFE041EDC0267AF1D67A
SHA-256:	133A201053B5F51BC75E333979E84C2CF74008642E6B7724DE3E03951FA368AE
SHA-512:	9E208BF8CA717067325992C4D097784B9CA554E1A893EE2701AE33E98FFF55BD138440C6493618D6F518EDDBCC9FB1B8ED1664FB615AD9C8B8C1883E6865AEC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel24_3Up_Footer_Surface.jpg?version=7bcc912d-1a61-9307-f613-1997da2a573e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_Panel24_3Up_Footer_Surface[1].jpg	
Preview:	......JFIF.....G8..T.'....:...O..}!K.cd.".4...>. P.U.....Q`.6I..u_}C.+....r..N..+.bK...C.%M..9.....g..m.M+7q.....*....k.]v8%.EY>..Q#e.../7?...x.6:.'&.<..V..^.ZW..#....$j..j...:)...\|Y.k.....n:l...\...qc....+.=.....].b.....7.....X.q/...Z.. .....^.. .!..GI..nV...q...\|...._';...v...^..o.y.BLq...v<lT....z.g..}j.b..'...z.4..HJ.9WO...<..FA..E..p...NBR....e....sm.;...U..Xn.....~fX$....[w:.E[....]....]Hw..}6.....<.....-../377.."...r..q ...@...7....Y...6.zx....V.t.....[k.....').....-.>.k.....d.3iw_.....!x.]..V...y.t.(....k.....7..S%..5Y.I.....Ix,.H.cY.../.@.i.g.+...k..Jk.Ix.....&m..XV..q.....ky....4...>n.4.sGL.1....j>...j._... ..!..Vs/.y.&.J.;....H0Uk.+.....cSn.=l...\....T.<.../..0....p.....V..._.&..8.-u.c.../.0"...[....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_Panel2_LinkNav_Devices_Win10[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1167
Entropy (8bit):	4.500982301012084
Encrypted:	false
SSDEEP:	24:tzS64wjDuIVilIxHsOYsblx41S3siZItiQyQX1qyU9F9602Eo3BR4m5S:hXLuaY+MO7bjM71C+8ojP5S
MD5:	203A9C57827F84239C05FBB71AEC5F76
SHA1:	495C2F881E909BF96ABBCA956BD43D1E322D6EA0
SHA-256:	93FB195EBC9A97EC5FFDEAAE219223E19277182C10829976411ECE6D28662A42
SHA-512:	94EFCD3975FE8ABDA444EEB45A9F0FCE624AB48BDDBA254EF9A40FAEF7F237723066DAEBC00F5AC2979E21C073D1885BFC2AD75843C529342505D97FAE4864 9D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel2_LinkNav_Devices_Win10.svg?version=377d6ae5-08d0-4d08-8a43-59dcd4acf360
Preview:	<svg enable-background="new 0 0 64 64" viewBox="0 0 64 64" xmlns="http://www.w3.org/2000/svg"><switch><foreignObject height="1" requiredExtensions="http://ns.adobe.com/AdobeIllustrator/10.0/" width="1"/><path d="m50.05 39.285c.145.144.277.329.396.557s.218.469.297.723.142.508.188.762.069.478.069.673c0 .326-.069.638-.208.938s-.327.566-.564.801c-.238.234-.508.42-.811.557s-.62.205-.95.205h-32.934c-.33 0-.646-.068-.95-.205s-.574-.322-.811-.557c-.238-.234-.426-.501-.564-.801-.139-.3-.208-.612-.208-.938 0-.195.023-.42.069-.674.047-.254.109-.508.188-.762s.178-.495.297-.723.25-.413.396-.557l4.117-4.062v-15.722h27.867v15.723zm-1.583 2.656c0-.052-.01-.127-.03-.225s-.047-.195-.079-.293c-.033-.098-.066-.192-.099-.283s-.069-.156-.109-.195l-4.018-3.945h-24.264l-4.018 3.945c-.04.039-.076.104-.109.195s-.066.186-.099.283c-.033.098-.059.195-.079.293s-.03.173-.03.225l.06.059h32.815zm-27.867-7.441h12.667c0-1.38.264-2.679.792-3.896.527-1.217 1.25-2.278 2.167-3.184.917-.905 1.992-1.618 3.226-2.139s2.55-.781"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_Panel2_LinkNav_HelpMeChoose_Win10[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	2499
Entropy (8bit):	4.145286575041427
Encrypted:	false
SSDEEP:	48:hXBDPbKtEkwWBPwl3nX2hjYhduOmfQ5pAUiBSzycF:RstEIBPwl3naCeFotF
MD5:	C995AB370737A85F1F2B6F1739EE7077
SHA1:	00623A7B72F4933A002628868790B124054B3141
SHA-256:	80A5896A0FB0D209C0303FD5BE3F686B7727F7528FA067E1E0D6CCB276BDAD58
SHA-512:	5C9952C381508CBD8BFE45D898B967135D32506D88B4A02B7CA27899FB27B43D6738D2328137D1EEC18656EA644761BD73FE076D0D7BDBBBD46A94A347FC075
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel2_LinkNav_HelpMeChoose_Win10.svg?version=7e9d3a36-d09c-42ea-54b0-380404a2167c
Preview:	<svg enable-background="new 0 0 64 64" viewBox="0 0 64 64" xmlns="http://www.w3.org/2000/svg"><switch><foreignObject height="1" requiredExtensions="http://ns.adobe.com/AdobeIllustrator/10.0/" width="1"/><path d="m46.625 25.143c.469 0 .908.089 1.318.268s.768.423 1.072.732c.305.31.545.673.721 1.089.176.417.264.863.264 1.339v10.393c0 1.476-.296 2.777-.888 3.902s-1.377 2.068-2.355 2.83c-.979.762-2.095 1.336-3.349 1.723s-2.543.581-3.867.581c-1.102 0-2.06-.065-2.874-.196s-1.538-.321-2.171-.571-1.201-.562-1.705-.938-1.008-.81-1.512-1.304-1.028-1.042-1.573-1.643-1.169-1.259-1.872-1.973c-.375-.381-.756-.762-1.143-1.143s-.768-.768-1.143-1.161c-.82.381-1.635.762-2.443 1.143-.809.381-1.617.762-2.426 1.143l-2.021-4.446c-.773.786-1.55 1.562-2.329 2.33s-1.556 1.545-2.329 2.33v-25.375l15.75 16v-12.767c0-.476.088-.923.264-1.339.176-.417.416-.78.721-1.089s.662-.554 1.072-.732.849-.269 1.318-.269c.656 0 1.198.113 1.626.339s.768.524 1.02.893.431.798.536 1.286.173.994.202 1.518.035 1.048.018 1.571-.027 1.0"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_Panel2_LinkNav_Learn_Win10[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	445
Entropy (8bit):	5.2124097142399695
Encrypted:	false
SSDEEP:	12:ty0Se14wj6Eq9UTZABQ00q2LtcwTNIUUQdyM:tzS64wjIU8ZeZeM
MD5:	792C8C8348A6B6C9C4D0C5B3C4060960
SHA1:	8D9938AC1F2E8F0D0F7B1AC6D1864EB6570FACAF
SHA-256:	14FA7C030BDA8A06A548DB5427394C8B838B298189320EACC395E6D2A53D5FAA
SHA-512:	B852CB7D335B6E96986315A565ECA925878E5EBB718EA1F9DD62E34630A6931F1D3F633D16715ED452DC7DE3E5834C5C65A38FE1F58C302AC1BC10240B7DCF5 7
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_Panel2_LinkNav_Learn_Win10[1].svg	
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel2_LinkNav_Learn_Win10.svg?version=3183f761-5af1-b793-95f2-9d593ab0f261
Preview:	<svg enable-background="new 0 0 64 64" viewBox="0 0 64 64" xmlns="http://www.w3.org/2000/svg"><switch><foreignObject height="1" requiredExtensions="http://ns.adobe.com/AdobeIllustrator/10.0/" width="1"/><g><path d="m30.577 31.383h16.923v-14.883l-16.923 2.364z"/><path d="m29.373 31.383v-12.351l-12.873 1.8v10.551z"/><path d="m30.577 32.586v12.553l16.923 2.361v-14.914z"/><path d="m29.373 32.586h-12.873v10.589l12.873 1.796z"/></g></switch></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1920_Panel2_LinkNav_Support_Win10[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1572
Entropy (8bit):	4.337612931532727
Encrypted:	false
SSDEEP:	48:hXKQxgL14FmX34y6mdUmnlWAeSDyCEXanaNQR:RKQxEEgplWAEhaaWR
MD5:	DEC312B88B1DE3A87A6966F64A3CAD21
SHA1:	6C2A02A86B2CE360EAA763B0B5C7D393A1CD6D37
SHA-256:	EDF11515F06316F47B01E94348814842BA23E7B051F1A851D3798530C66EFC56
SHA-512:	9390112CFB4195ABA89DEBA391993A8B801D89AE3A622036255FADFB3EAA4E815EE8347E5FEB9E84545A78E7789E7F6FBBF26309DF6FC2C72F6CA1B5DB083F05
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1920_Panel2_LinkNav_Support_Win10.svg?version=718bd6b7-9e32-091b-115b-89c8ba522fdb
Preview:	<svg enable-background="new 0 0 64 64" viewBox="0 0 64 64" xmlns="http://www.w3.org/2000/svg"><switch><foreignObject height="1" requiredExtensions="http://ns.adobe.com/AdobeIllustrator/10.0/" width="1"/><path d="m43.855 23.598c.107.457.191.917.251 1.38s.089.929.089 1.397c0 1.734-.325 3.311-.975 4.729s-1.59 2.736-2.818 3.955c-.99.984-1.751 2.06-2.281 3.226-.531 1.166-.796 2.446-.796 3.841v4.5c0 .469-.089.908-.268 1.318s-.423.768-.734 1.072-.674.545-1.092.721-.866.263-1.343.263h-4.581c-.477 0-.925-.088-1.342-.264-.418-.176-.781-.416-1.092-.721s-.555-.662-.734-1.072-.268-.85-.268-1.318v-4.5c0-1.395-.265-2.675-.796-3.841s-1.291-2.241-2.281-3.226c-1.229-1.219-2.168-2.537-2.818-3.955s-.976-2.994-.976-4.728c0-1.137.149-2.232.447-3.287s.722-2.039 1.27-2.953 1.208-1.749 1.977-2.505 1.619-1.403 2.55-1.942 1.933-.955 3.006-1.248 2.19-.44 3.347-.44c1.646 0 3.221.299 4.724.896s2.845 1.465 4.026 2.602l-1.61 1.6c-.966-.914-2.064-1.617-3.292-2.109-1.229-.492-2.511-.738-3.847-.738-1.42 0-2.756.267-4.00

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1x1clear[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.122191481864228
Encrypted:	false
SSDEEP:	3:CUTxls/1h/:7lU/
MD5:	F8614595FBA50D96389708A4135776E4
SHA1:	D456164972B508172CEE9D1CC06D1EA35CA15C21
SHA-256:	7122DE322879A654121EA250AEAC94BD9993F914909F786C98988ADBD0A25D5D
SHA-512:	299A7712B27C726C681E42A8246F8116205133DBE15D549F8419049DF3FCFDAB143E9A29212A2615F73E31A1EF34D1F6CE0EC093ECEAD037083FA40A075819D2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/_h/9be151e5/coreui.statics/images/1x1clear.gif
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\4b8d9e30-e1b0-4027-80e8-74da19dd38b3[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 539 x 300, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	11870
Entropy (8bit):	7.880799221591595
Encrypted:	false
SSDEEP:	192:+cuRyUFYbH2tRJ2CaMEukCP9o97V+w5MBZ+7SHDbVJLvrLmzMa3eMV5laVegZlA:WHFYSaukLN5MBzLSBVAeOS
MD5:	3D4354495BC140D6D707CF5CFD67561A
SHA1:	3D2E725340F89DE95BCA8D32FE922316C8CFAF0F
SHA-256:	E2BA75CD68317EC896F72B2EE95515FADA7E72C1F6D88AF9CD68AC2E5A25D848
SHA-512:	A8AC6D99A8367E3BEAB36E5362B3E7E6CA3657AD11282FBCF7E3DA76C4B20F716AC8D5C5C64CB93A7CE0E2AF11AC1F5CB6AEBA63A640CE18EAE8735E9C4D8370
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://compass-ssl.microsoft.com/assets/4b/8d/4b8d9e30-e1b0-4027-80e8-74da19dd38b3.png?n=539x300.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\4b8d9e30-e1b0-4027-80e8-74da19dd38b3[1].png	
Preview:	.PNG.....IHDR.....,.....j.q5....sBIT....|.d... .IDATx...y.\U....u..tw.I Kg.$]U..H...#Q@TD..GVap..g~...:.@.Qg.\.AGGA....PG@.....Y:I..V.U....N.^...~..'.{..&t.?}...+..... .....QSS.W_z./.].....].....9c.....]...`...@yhnn..Z.....<.a.u?x.F...@icf.....4$.u].c....y..Z.Wm.J.3. .F.q...%]>.uk....d....-..}x....D.%...`H.6m..y.$.:.1===..b.$kmO<...h4.j...b.....6....+....4u..<.SWWW.....S...../.U.....z6.....>.....Q..$9..@ ..@ ..O<....~.=.....7.....e..7.....wvv ...7..h^..P....F.....k(....k.....a.zg7.....q.....O.o..s?.....~4}.....Sss.[.....I...B..c..u.KSS....e.Y..8.XL===#.....;..+W...J..O<....&M.4k..W…_n.}s$.y...RD..F....Uc..)/.".vc.C.P...h nnn..~Q.....Z....t.k...w.....|.=.....===.&N..0e.K.....T_YY).qn..._.F...6..455m7.....;.socc.o.ZT.6l.0.q.OJ.;I.....[.x<.c=.....r..>..c..#.n..Vg...=.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\MWFMDL2[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 9040, version 0.0
Category:	downloaded
Size (bytes):	9040
Entropy (8bit):	7.922230355841189
Encrypted:	false
SSDEEP:	192:4yUhlPlzn894zIJ3gAIsp7bBhjiFBjZzTJC2IQhaXZYDFGs:4yUH894zW3g+3WHeQhmYJL
MD5:	DEB7F918A49E8C00FDA777266BCFCB8D
SHA1:	9E830D7AE16C3BBF644838C88EC9E7C84846B77A
SHA-256:	7CF14745754DFAC5553A8F4442FF6B92A0DBD27BBC134A6958A9D72CEE1071FB
SHA-512:	15394C1485FEC66AEAB7A147B2ECCA06B8B6FE74BFCE351D431651DFED5FB24B65B46330B58EC755874323D27A17B0B9B757CE5F9C727897725853C3519F505
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.onestore.ms/cdnfiles/external/mwf/v1/latest/fonts/MWFMDL2.woff
Preview:	wOFF.....#P.....<l.....OS/2...X...H...`JZtEVDMX.....^.qcmap.....O.....k.cvt ..... ...*....fpgm.....Y...gasp.....glyf.....R..(.C+.$head...h...1...6.. khhea.....$....hmtx.....]....$...loca.....~..9maxp..... ... ....name.....I.post..".....  .Q.wprep..".....x...x.c`f..8.....u..1...4.f...$.....@ .....o58.|...V...)00..... Xx...S....._..m.m.m.m.m;e..y.~.....<p..a.0t.&...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...].na..G.3.....}.~a.p@80.....C.a..pD82.....c.q..pB81..N...S.i..pF83.....s.y..pA.0\.....K.e..pE.2\....k.u..pC.1..n...[.m..pG.3..... {.}...@x0<.....G.c...Dx2<....g.s...Bx1..^...W.k...Fx3.....w.{...A.0|.>...O.g...E.2|....o.w...C.1..~...._.o..08.....?..0$.....x...+.q.....1.....R...b9 ..qg?23....).$.....8.2R~$Y.i...|

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Prefooter_Icon_PowerCord[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	302
Entropy (8bit):	5.351026925841641
Encrypted:	false
SSDEEP:	6:tvKliad4mc4sl3QQkaguXABNPX9KRdbBRFW7AS9KRpg4714SBG3jppXT:tvG1jkGAr8dbBRj2KC4715BGTppXT
MD5:	C2442C289BB7C58FF328F2482C0F5DA0
SHA1:	19919649BDB860CCB297CD5723F08DE8DBD153C1
SHA-256:	0637D2B9FB19C88EB4764D9BB21A900FB43BEBE7C78C9A729D8DF3F7C9AC7BB7
SHA-512:	B362AD67C8EA3804BBBFB1B9EA11A918B88F8289D21BD634EC4F784AFD43098060F23EBDC4AF903B7B9AA1F15077FA46E7771C7C68C3A1ACC98248058B76CB 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Prefooter_Icon_PowerCord.svg?version=3d41ef0f-fcff-4126-0dfc-499e388476b3
Preview:	<svg id="Layer_1" data-name="Layer 1" xmlns="http://www.w3.org/2000/svg" viewBox="0 0 50 50"><defs><style>.cls-1{fill:#2f2f2f;}</style></defs><title>Prefooter_V ectors</title><path class="cls-1" d="M25,9.06,40.94,40.94H9.06Zm0,4.75-12.5,25h25Zm-1.06,8h2.13V32.44H23.94Zm0,14.88V34.57h2.13v2.13Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Prefooter_Icon_Register[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	4851
Entropy (8bit):	3.83658682501437
Encrypted:	false
SSDEEP:	96:STdFYr7z6LuoWv0kLjGf4y+YiUPfthwMMvf+bzvrBCJ+XaaeRm3LfNk:SQr7WSfZjG9i0y+vVCJ+QsLfy
MD5:	E2ED0EF2A31F5039FCE16F6D66B026B5
SHA1:	017FDFADDB99F63BE69A0E4132CAA99FD1488187
SHA-256:	937A8643E73862DB96407B48C64F71201B08B583B941D291CEABEBAE878DB769
SHA-512:	914B88110497588B200B4EF359BCEE5B4063EFA7CCAD8F220C2F5B66B5EF277DFE2AB58EF6D09C29987FD818731E1C0361F81477A752932F34199466EAE0FBE7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Prefooter_Icon_Register.svg?version=0956d5fb-33ca-bdf9-3cab-37dcadb07379

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Prefooter_Icon_Register[1].svg	
Preview:	<svg id="Layer_1" data-name="Layer 1" xmlns="http://www.w3.org/2000/svg" viewBox="0 0 50 50"><defs><style>.cls-1{fill:#2f2f2f;}</style></defs><title>Prefooter_Vectors</title><path class="cls-1" d="M25,7.5a16.93,16.93,0,0,1,4.64.63A17.82,17.82,0,0,1,33.81,9.9a17.7,17.7,0,0,1,6.29,6.29,17.82,17.82,0,0,1,1.77,4.17,17.34,17.34,0,0,1,0,9.28,17.83,17.83,0,0,1-1.77,4.17,17.7,17.7,0,0,1-6.29,6.29,17.82,17.82,0,0,1-4.17,1.77,17.34,17.34,0,0,1-9.28,0,17.83,17.83,0,0,1-4.17-1.77A17.7,17.7,0,0,1,9.9,33.81a17.83,17.83,0,0,1-1.77-4.17,17.34,17.34,0,0,1,0-9.28A17.82,17.82,0,0,1,9.9,16.19,17.7,17.7,0,0,1,16.19,9.9a17.83,17.83,0,0,1,4.17-1.77A16.92,16.92,0,0,1,25,7.5Zm0,32.81a14.75,14.75,0,0,0,3.81-.5,15.68,15.68,0,0,0,3.53-1.41,15.41,15.41,0,0,0,3.08-2.22,15.62,15.62,0,0,0,2.47-2.93q-.22-.51-.43-1a3,3,0,0,1-.21-1.09,6.77,6.77,0,0,1,.06-1c0-.26.08-.48.11-.66s.06-.35.08-.5a1.34,1.34,0,0,0-.06-.52,4.09,4.09,0,0,0-.3-.7q-.21-.41-.62-1.06,0-.12.06-.32a3.46,3.46,0,0,0,.06-.43,3.6,3.6,0,0,0,0-.42.71.71,0,0,0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Prefooter_Icon_Support.svg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 63 x 63, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	590
Entropy (8bit):	7.495068343701629
Encrypted:	false
SSDEEP:	12:6v/7p6Nl6GVlwl0kGIRdL3AOzg5nDh0LoW5D89+GLHJhLtUOAKb4JN2+G:86XZl6GIRdLnzunt0r5D85LpYKb4JEX
MD5:	49A1F0189748EDE3AF29BB60606C22BD
SHA1:	D319994CDECAC4D85240DE6CC285C164FB5BB2D6
SHA-256:	3CF56E5D0FC1564FA5DF5F8FC7792207B8B6A00179EB71330B5E08479962C83D
SHA-512:	7A42843975F190664D0652C328E9523213D7B6A03EBF4048B318A24D69DA7C2396AA501B4D74C069029AE1AB972F8273D3C01CCEA609BB7BD6DBEA3C3BAF374
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Prefooter_Icon_Support.svg.png?version=c9732530-8f2c-4147-d343-fb2ccf2e43e4
Preview:	.PNG.....IHDR...?...?.....V.T....orNT..w.....sRGB.....IDATX..[..0....X...b.....X..X....C...{6.sf.....=.7..... ...Xa..X...-Z;..ZAm....h....a...f.....t.t.y....G...=...U..=.IpF.....B...'Ju3^.9..<M..3e...0.....u1....`..y....k~.....0...s.Mi..u.m2..A....Ub.....W.....*.;.w.....^."..P....;.@...xW.|f{...?.d..v8.....k..O.%.".e$....w..sT.V.W..N.>..E...s.....5..Y.t.2.....x.L.gI.2FP..L.xZ+.....hd&.|..^.. ...8F.....o="0..+[.W.)p+.-..v....B..x.....uT..^?..../.#..a}~&...u.0...ru.y.....5.....2.JP....w.. .Z.<.....^..*".....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RE1Mu3b[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 216 x 46, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4054
Entropy (8bit):	7.797012573497454
Encrypted:	false
SSDEEP:	48:zICvnyRHJ3BRZPcSPQ72N2xoiR4fTJX/rj4sFNMkk5/p1k2lPUmbm39o4aL7V9XH:10nvE724xoiRQJPrjpLKSFl9oX31Z1d
MD5:	9F14C20150A003D7CE4DE57C298F0FBA
SHA1:	DAA53CF17CC45878A1B153F3C3BF47DC9669D78F
SHA-256:	112FEC798B78AA02E102A724B5CB1990C0F909BC1D8B7B1FA256EAB41BBC0960
SHA-512:	D4F6E49C854E15FE48D6A1F1A03FDA93218AB8FCDB2C443668E7DF478830831ACC2B41DAEFC25ED38FCC8D96C4401377374FED35C36A5017A11E63C8DAE5C87
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE1Mu3b?ver=5c31
Preview:	.PNG.....IHDR.....J.....tEXtSoftware.Adobe ImageReadyq.e<...(iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c132 79.159284, 2016/04/19-13:13:40 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:A00BC639840A11E68CBEB97C2156C7FD" xmpMM:InstanceID="xmp.iid:A00BC638840A11E68CBEB97C2156C7FD" xmp:CreatorTool="Adobe Photoshop CC 2015.5 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:A2C931A470A111E6AEDFA14578553B7B" stRef:documentID="xmp.did:A2C931A570A111E6AEDFA14578553B7B"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.....DIDATx..\..UU.>.7..3....h.L..& j2...h.@..".....`U.....R"..Dq.&.BJR 1.4`$.200...l.....wg.y.[k/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RE42xlI[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 400 x 120, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	16004
Entropy (8bit):	7.975327533302786
Encrypted:	false
SSDEEP:	384:T0Cfurr1lToyZdUGnXbUC9Mk+GlrqDdhoMtRftG/:T0OurDsyXUyUCr0SMtRftU
MD5:	05B6F8C8468A1DF2FC32176C3DA7CB79
SHA1:	45436C5ED82D11499A8FC9FAE97971021D2B18A8
SHA-256:	2F44F1F6E1B20E3552EF58ADDFF0FEE62EE2254038C383ED83EF8A667E2C8CED
SHA-512:	074BDEEA5D8BB3720DD7964E238E6EE6DEAFA59947AB4CED28AB81482C0DE77303426A675F23DB6EC7209C61A1669DB46885ADD6A224E1F620F0C69FDE51822C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE42xlI?ver=6ec6

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RE42xII[1].png	
Preview:	.PNG.....IHDR.....x.....>KIDATx.....`...(.... [.q..D.s.l.n....d7..h.....=>...../^.`..3gF.i..9..`.....M.t;).HV..`...=S*.)._.....z.P..*.k0.Rm.P.&.2...HI.% S.Z.2.R5.U..E.....J.....2.q.~..L.4e.p..r`._.N(...}a..=.....#G=?p.p..+J.2.^.F./_..1b.....{O...UT.v;r....$J..g.F....h..x.dYF..m..u".cD..o.V...P..W4n.....JDQ..(.(B....O.s.\@.....1"..F @.....'d{.....8..H.^.2c1KWn....gm..Z..;kQ*.s....$M.....?}&..1 !'M.2.....2.....q.V..''(....y.2.T8qe..'l.{g.#....s...._...?...J..zAT ..R.S}.q...2I..._...SH....?.....z.....X.....s.....q...0.#..k..J ....}..H#m..@H^ ..D~.....W.....y0..p...*.BR.@%."$.A.....%..N_..9...#.x}....g..nx..<W.$Q.qR ..m7`R.4\..$.B.}...j.....u....Jl&.hY.~....p...".O.#...Sz.H.0..\.....1..w...z,r...j..... ..,?....&.rp.a....L...J.H..i..A..p.`....OU`.....$..v..f.A^@:./...:1.Ha<.a<...8.{...5."]$.5...-.....,v.c{v.G..m..g"^K...^.g..>~.....# ...d!|.@h..h.]6...RI..5'.=..*B..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RE42xmN[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 400 x 120, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	13967
Entropy (8bit):	7.9486760204482465
Encrypted:	false
SSDEEP:	192:9LiHlllc0s75+zd+atHN8jiffaYpxs4M72glZkVasaMPqCorG5aGTyntPv138XPx:ilzol35Vxs4MKglZ3MCS5a8y1vSJb5R
MD5:	11A868843FA0A7CB1E9C383694F8B6C1
SHA1:	9227405267EA296EB6F3D12F744814B6DE36C185
SHA-256:	8A422BE7343A097C608112FD29EA309201101816627C3D7EF0F8C95BD3936951
SHA-512:	E22D9479D90FDF27BAA9C289A20844D8A0FAFB3F1A1594362F8198FC6A4BFD6971EB7AD949F2EE06F8BECE8FFD4F9D8734F3D28B62858CC2CCFD7F2E7FA6CI C9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE42xmN?ver=52e2
Preview:	.PNG.....IHDR.....x.....6VIDATx...A.....iC.r.....^..={H.+.....mk+.BG5.....Nj.jG..mc....D.8....Vz[.....O.....g.....B.(....`(.e...|OJy...3Ms...'.....pl.._....,.IX.....9..b... .Rj....R...2..^o.,..c.....Z...x... .....X0..!...\,+-w....B...4.=.;..FQ(....Q.$.....b...".k@GG..?y...1.....}..... .'hz....!.....RjW..q ..7..q]w!..!.....]....Fo__..X~..y.R.....0.....P(bm}..... .xvc}..'!.i...C.I&..R.m.....@k....z Pj....:.....j$Y.....B...f.u...).'..?.8.133...$...,Y8b.6.[..:.....4...}.nw..o.w..[.[.\....hll.P(b..a.s..TI+%.R..Z.Ul.H.4....]{.9k.K...;.....Z.....9.|^ A ... ..g. z..V...b...W<....B..k...i...`.D.E444.....W....I..D.Q.....\k.....].jc.....}...o.....G...y..'?.e/;d%0. x.I.F..]..W^sM....>....V..jU.....)[.....r.PWQ.BR.U...Q....&r.....lH..*n. ..B./ .V..~Lc3qe....(J.....c...x.....n4.. .5koY....b...<..Y.}f.....c..R..Pl...9...OEIZ.:..V...Q...Ut.k.S....^...6...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RE4FP42[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1038 x 691, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1994017
Entropy (8bit):	7.983659064488733
Encrypted:	false
SSDEEP:	49152:Ke8yW7+ag3jqbIGou7OgdvtZzp7pS17Synf3wBN40ogppJ:K5yxag3jqFou7OgdVZhCzfw80ogn
MD5:	3A66F563240021543DC98085DE47D821
SHA1:	51AAC21266499E1B0DBBDF2DFB9789557C848309
SHA-256:	ABCD2A1F3BB7C9E2636E1BF6EF7E7ACB1DF3719B53188FA2D2E5C093141086DD
SHA-512:	4A8DF738BF08B359753CE1B36A008E0219B27312EED7975F05FDEDF67C711EB1EF99CAEED07BFD70E7223AE9F2059766B82D4024A100E1E4FB474C6EAE65AD CB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4FP42?ver=cac2
Preview:	.PNG.....IHDR.....ZO.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^t.....6...x...;.$f.c;..CdI..%Y.eI.3.iW.]i..effff...effA.....S=.R.....TUWW...T...sN..!.a.-.Uj!..J 5..RE...&.R*.7..=.Ke..RU..T.j.U..H..wI..J..).....6'FR.eK..ji.])M.h..6i.[#Mt(...FiL]MR).k..1U.4Az..^..PHs..i..Q.n.....\|..4^j....r.../.O..0D.-.....0.'?X....&Uy...t..A...(]....i^.'...J.Y. .@A.4X.,...H..^Rk..... .....\..H..R..Q)....dw...rV_.s4.".d.q1...-.D.K)..ZJ"..a%%{[K.^6B2./H...RIr....(Y..&.[.... __.^{..../.Yz.J.....k/K.....}....m.%.#.%..$.C.I.{...w....}!.n_-.o[%...3I o....>.Nm.L..J:..3..O...v...-.P?Y.../.?."...Y....s...s..O..^%....I.B.Y.o...~.J:.....V...%..Z...i.....U$_H{.\|d.W._..N.X'....t....IGI.....I..z*.+....8v\|.w..?H....~T.^:N....t...../..?.%Y# ._8%).$e..T..).zJ).g$.....6.../...H..H...)...j$%:.K...R^....m).9.Kf.J..~-9[..L..a".F.He.g...G$.....lw.3.]....c...H.)#.\.t:Jr\.>(Y..B....y.'..WK.v.....2.^j"..Zr.....R]....f&.l....Z:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RE4GG6p[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	4901
Entropy (8bit):	5.197679477689848
Encrypted:	false
SSDEEP:	96:AxtrMzrHG3wQreAjreA/nreA3xreABfrxpjoLUJtMyUJt1dUJtzaU8cBCRp8cK4W:A+XrAeACAYAtrxeLSMyS1dSzanQCRmbD
MD5:	C2808C1FFF8BCA99C899DC970E72967B
SHA1:	BAE8B1BFDB18B50A4CE1508EC20ADC56D08909AF
SHA-256:	82D7AD5F3EE6E54DBCD0FDB04CC54BBAAA34B6BB3033B9819A867ABCD33E0D2A
SHA-512:	7E19F303DDDECFDD47145562B8A0009E1529D56A991FC7DD8609E73F58458E614C60502B506C16B491E14E8D2A5BA2DD1CB700FA7D0A1854CFA2466877BBB3(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prod-video-cms-rt-microsoft-com.akamaized.net/vhs/api/videos/RE4GG6p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RE4GG6p[1].htm	
Preview:	{"captions":{"en-us":{"url":"https://prod-video-cms-rt-microsoft-com.akamaized.net/cms/api/am/videofiledata/RE4GG6p-enus?ver=f618","link":{"href":"/vhs/api/videos//captions/en-us","method":"GET","rel":"self"}}},"transcripts":{"en-us":{"url":"https://prod-video-cms-rt-microsoft-com.akamaized.net/cms/api/am/videofiledata/RE4GG6p-tscriptenus?ver=942b","link":{"href":"/vhs/api/videos//transcripts/en-us","method":"GET","rel":"self"}}},"snippet":{"activeStartDate":"2020-10-13T23:03:27","culture":"en-us","supplier":{"name":"","source":{"name":""}},"thumbnails":{"extrasmall":{"height":0,"width":0,"assetId":"RE4GScv","url":"http://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4GScv?ver=b6fa","link":{"href":"/vhs/api/videos//thumbnails/extrasmall","method":"GET","rel":"self"}},"small":{"height":0,"width":0,"assetId":"RE4GScv","url":"http://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4GScv?ver=b6fa","link":{"href":"/vhs/api/videos//thumbnails/sm

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RE4GyKc[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 400 x 120, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	18381
Entropy (8bit):	7.9792625595650435
Encrypted:	false
SSDEEP:	384:aCXj0xWxq4dpQax0gA6TnJcamFq1q5yNWiG2UB67NNA:ar2Uax0gxnNmF46yNi2UBwY
MD5:	05B38E0772D2F120BB5B9E38696B7D4D
SHA1:	547D26C57F77A703FF8426F5A6595756FD279417
SHA-256:	C6EB313F5573328DC784D5689298218E4D3C8352951DA8A7FBB9C4317F0B75A3
SHA-512:	F02C68D52A6015B48AD21BB1C68272D2717F20D5151A6B4BC290481C2C05275061D3F4D10ED1412A63DF885758E232E97B20F185D58C277A6EC5A11D7E8C0D9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4GyKc?ver=f8b8
Preview:	.PNG........IHDR.......x..........G.IDATx...A.@@..0.B:....=D...Vbq.7.$........jY.'u.7MU..{,..E..Y=....B33ff'ff.....2sh......A.sM5z..g.d._...&.n..].....76....A`....@...\|D.v.Mb..)..cn......3....4V.g9.45$.9....h...}..\...1.H.O...w.-...'{.M..c;~....?.A.x......W.C...........m_..W~..y.]w.....#...g|.].x.._0C...76.N.........g..[..7...x.S.....A.........g?......g.Kp.;..<..lo.=...9]e.(..+..j...cTl...R.YD.Ue..p...4..Y.r.....i...\.4A...[.)..w..:.cM.G.....g_.2....g.{..c.U:.=X|...f.Ngk....y....y-.{.S...D...LP.......|..'.)......*.6....jE.".M....C^G.7J68.v.N..3..Bd<..87p.{<..=.A.#..7........,..V...9w...................&.....Q..{..RK%...s..$HB.]..w..C.o.8\|.&...LR0.F.U..m.~..]..h4lm.f....>Z.......Y,.+....p9........)dk..i...].....h{..0Neh.......$..Hc.K5Ii.&...i.1.Q.&;..`......."H..U.-..D..&.H}...t.`.@..R-g.D...."..K....,*-.A+...A..p....)A.!.bP..r!6......I.#.Hs:..A.2...#s...84 ..~H`.j.A;w:..F:..J..3.E.G...dT.w!..4..,P..5.#C..(g0..Xd{.{....w.Y.V......1.04.(.B...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RE4hgqN[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 359x234, frames 3
Category:	downloaded
Size (bytes):	3464
Entropy (8bit):	6.8572628048727395
Encrypted:	false
SSDEEP:	48:BGKuERABs+ddddddddddddddddTFTvAzfJW0MdHW8Gu4Fjdddddddddddddd53m:BGdEVwFTvIR9sMsuBrLqJ9Y6r
MD5:	A33C257477A176B69241EC416CA74160
SHA1:	3DB79476AF74637111206FB26A77F3A1221D4E9D
SHA-256:	A3A8A262F6A5A57F517E7E362A45C727F61EFC6FC6B98DE3BA3BD29DBEBE65BD
SHA-512:	6918D084CED2141A4AABC52D4A1409F7AD563A8D98976E6E477706F2965D38BDD3EB0F48153BB3C7CB0EC5364B78FF40870FFCFC7561915182CDD5C00F2A4A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4hgqN?ver=26d3.gif&q=60&m=6&h=235&w=375&b=%23FFFFFFFF&l=f&n=f&f=jpg&o=t&aim=true
Preview:	......JFIF.....`.`.....C................ .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO........g.."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..?...(...(...(...(...(...(...(...(...(...(...(....n.m....H...h.#..l....z......o5..H....O.@..E..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..QE..V.\|3.x...c."S...O...7..37.uQ.-..Xi.....5..}...e...+...*...>.......=-U..}......d....-[L..N....5....o...M..m..m..%....^Qw.\^H^y]..ri6R..T......xn....kn.P.5..ha.L\|.H....$n..5.._.cq..$.A.Ts2...Z...]

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\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+KloofIhrVvMaESGZM0JXgOCrYX81Gx8I/x9AoQYJNZ:e+KoNhr61Sy348xn/36Af
MD5:	996AF36AF03A6BFB1654B69FC907A31B
SHA1:	1724A4F1DF9BFD5426111A0C2A7699EC52E549C6
SHA-256:	1CF63BEC6AC27FB198DEB2DB704602465A5AFCCED262F17C3F656D0FC1F0C37B
SHA-512:	8CE3C41F2FAFF99441A2374447B2091EB35E91239CB5D59C2D6EC1775037CC57BD0839FB5AD41FF32AFE11A3BBA3CEC9872765FCFCFCEFA0BFA62F719B5E851A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RE4qZpg[1].wdp	
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4qZpg?ver=06c1&q=90&m=6&h=180&w=321&b=%23FFFFFFFF&l=f&o=t&aim=true
Preview:	II.. ...$..o.N.K..=wv.....A.....$..B.....$..B.....H.....WMPHOTO..E.q.@..0...,8:B.. .....;..9h..... P.T....,0`.!...k.9"Jw.,)..iX`..0 .+..lru.2.k..1.9.. .0 nk....J.].6...6I...R.9^....W...S....x,..|..3..3.v.b.:.....K.4...,..M..:.-!..E.U.....u.Yk./N.(.....x.....Q...v.....!...2b7&"....(I>.w.[L.....%.I.6.....T&.....G...v.&...& .+aE.'...2.$'S..M.tn...u"!.f..e.^....8.(.\,H.....H)..q.O.I.M$k']:}.i..w$(.S..#J8.=%p#@vo/.. .P..c..$.8.Z....I^/....`H.E.....Pu..I..B.../.Uu.....&..!E..I*.(..E7...2*.../+@i!.G.'#.Q...?.&.}.H d...+.Z7...\.d..+&U|....v..R(u:...A!...Zl...,.....Fg.!..M .|....#~..`.p...4F..MNF.R.....kB#-.d.$.I.2.....#..nc.@.....Y.4...`...Z.\@... @....q..B@...{..@^.rqQ.M...C.z.I}S..H..E..Gh...P2f..p<. 5H..g.Q.I.s`V5$l})...Fcc.K...*r....C.\.Pt.+.P.T.LC...H..A...5.w.!..4.....5.\..5.E!.B8.;.+h...B.P?....7...\.....~|..O).CtX.P.M.j..(..c1|.\....iX.....T.c..o.@..$f-.2.@.g

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\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
Encrypted:	false
SSDEEP:	384:gXYa2gpV+kPcit03ncKOqM5lG7i55UCzb+yTBANXBa:YYajp0kPci2cKMJ+yTBANE
MD5:	66A22BD08B368DCCF91F88B464A2F06C
SHA1:	1655625A2BD547596D5911EFE6138CBAFD8148C0
SHA-256:	7A1646CB3FE1B2527559DD5A5DEB621714CCC7315B3C0041ABC057B3F6818A20
SHA-512:	6C408937D566FC880BDF262D9E1CE659AB198A5B815CA36CF716B9FFC5C2E2C9827EEB32167C2105966CED9639C0CE1B25C40C670C9974C6B3ED2877091155A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4r4UB?ver=3307&q=90&m=6&h=180&w=321&b=%23FFFFFFFF&l=f&o=t&x=558&y=161&aim=true
Preview:	II.. ...$..o.N.K..=wv.....A.....$..B.....$..B.....4.....WMPHOTO..E.q.@..0...,8:B.. .....09.....`....<..8P.4.....bn...D.M3....}.]- "..uBb...<"c.=i.#B.xu.9Rn.....zCH.."p|..Y..@3b3....6.....*.j.0;]."..... .....@.9)&.A-..a..A.>uD.....jx=S.B.....Y.-...R\."...Y.../.4..7Mj.M.....7g.V(.I.(.}.j4.Ad.:(b6..1...z...(.4..(.....Fl... ....".\.4..-7/..._s.ISN .S*a..-..,".8.....$].X.w.C.sf.p!hq.....S+."h...PH.'.>.\.....1.)...M.AY`.....&.".2;.....;.,..qW.:.xE..I.....*..Od..,b.}df.....Z..4W ).yx."....Q.M..vONL....*...I..... .1":4.X7"m.....0....4.....I.....FX.)HA..`!.....@..ELVrHY...U...A.DA.%.<6.....E.....rS.A0...$...c.._..m..... B.. ....(... .../.Vq...E.DA^4.D6B.....v<vSoH$.|."&C A..NA..i...@b.Q)....c....<.E...e....)q.`.jz..\2=..K%>.. i.1.Fc.....Y.1.45.#z.wTK.3...."..B...D.R..$[...G.X@O.h..J.....^.1.i.L.>...F....!.b..d...q..t.C...e.CR....#

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RE4tZqs[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	4491
Entropy (8bit):	5.209260121683626
Encrypted:	false
SSDEEP:	96:Axelre+Urre+U/Xre+U3xre+UB4rxpLLUMyU1dUzaULCRpg49Pm+MPfpecK89rZ:AL+UW+UC+U4+U2rxRLPyCduaUCR649Ob
MD5:	C3D7879D0FB0418D320FF5D19453521C
SHA1:	DE873A50F56DEC93EF6166FA55B0E8F28D76D501
SHA-256:	1C0D8EBE468DD136126D32FDB3B69E9BD002EA9CB7BB9F5D9A22C366C0BA5422
SHA-512:	34388328EBEEDC6142C589B6F8275A2D1D4FA721017F2AA5FEC8711BAA9956FFC0ED11CD511F6A10E3DA37364835D8F7838B2B0BD3CA38F5DFA54F2D820773F5
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RE4tZqs[1].htm	
Reputation:	low
IE Cache URL:	http://https://prod-video-cms-rt-microsoft-com.akamaized.net/vhs/api/videos/RE4tZqs
Preview:	{"captions":{},"transcripts":{},"snippet":{"activeStartDate":"2020-04-20T13:25:16","culture":"en-us","supplier":{"name":"","source":{"name":""}},"thumbnails":{"extrasmall":{"height":0,"width":0,"assetId":"RE4tWN0","url":"http://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4tWN0?ver=466b","link":{"href":"/vhs/api/videos//thumbnails/extrasmall","method":"GET","rel":"self"}},"small":{"height":0,"width":0,"assetId":"RE4tWN0","url":"http://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4tWN0?ver=466b","link":{"href":"/vhs/api/videos//thumbnails/small","method":"GET","rel":"self"}},"medium":{"height":0,"width":0,"assetId":"RE4tWN0","url":"http://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4tWN0?ver=466b","link":{"href":"/vhs/api/videos//thumbnails/medium","method":"GET","rel":"self"}},"large":{"height":0,"width":0,"assetId":"RE4tWN0","url":"http://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RE4yf9A[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 400 x 120, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	22420
Entropy (8bit):	7.980366544618822
Encrypted:	false
SSDEEP:	384:s+ZHeSW4mPxBdMafBW6EsCRIC6m1ApqzFvvLZo0UPbi2i1pB:NwX4m0UZpsSiLpB
MD5:	7770EA50C1F74B9C8B437DF7BAE41615
SHA1:	75E3C36CAA98358D0910D9DC99838C301F4F1C38
SHA-256:	C99E46243C0F2243437FC876B52528134276A79BB23F42F60E0A31D4638B46CB
SHA-512:	6939AE08FD68A5810F57D37A4AAA56639DEAA2DFBA02553DAD190542B112114A0763238E4420E91E52B25454BA9F61CBE4BA0B7B7CF7F4187252578DF8FCB7CC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4yf9A
Preview:	.PNG.....IHDR.....x..... .IDATx..y.d.U&.....R.U.U.U]..RkC.2...k..3...sl.....9.a..3....Y.....<....Hh.I-. ..u.....c.%..m>..~/.EVf....#.....+.~.....''..b.-..b.-..b.-..b.-..b.-..b.m.M..Q ....V.....S.\N~.....:'.x...Jn(@ .1...^ .~.....C.c.|<..:.=.~....}..L.....c.v..\..e...E.\...+PUup.~.@.4....k....''....iy.L....'}...o..!...@.u.\\.q.h{...v...KM.h..O.q.|5U....]........3...q.....<..;..8}.u\..<.u]....^.gw{=.....v.v\.n.Z.k..].z..e~9.....iv..5../.S.....q0..._...b;..y...#....{.T...1^..&...[...y0t.....i;...q..q]......=.t..r..t=.....|.....9s.u-..l..l...c..&..n....w,..q..K..-....:....k28.....|L.....C...L.H.....{..._.....|..j..7-.v}.....[l'..e..G..Lomm=a..9jr.v.....*J-....n.w:.).s.^.I..g(.Rw]Ws.7..yr....0(0X..w-....K'N.#.*o...{r.>.A.#...._.p..#I..H...B0....b..et%..=d$.....}(#..d.....0?...w..k....;.@...r4..k.b...bYp~....f..../.O..._~...l''.`.L.....t.YxGN.r...!...>B....G.4..|O. g.i..S*..7.J`...n38q~...C..^.~.,...9r..}.z

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ScriptResource[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	26954
Entropy (8bit):	4.516288580103467
Encrypted:	false
SSDEEP:	384:EMgviMjM4if38GmhXeC1QRwweTkBE9wbOY4Jf/JhRZ5h+73hNVt8oC4veONhLYVi:ZLEiJSdo11vIYHqb5Klo8v
MD5:	3DBD97A205B8CE59D755AB94F8C42964
SHA1:	B0520226342BBA131160A510BA3B57A1E8B7B80C
SHA-256:	36F7B9FE80A026A5D933855DE494AC6B7A4D01A93C26CE8A8737EED0C79367F4
SHA-512:	82BE6F1015CC346811EB736BD78F4949C855E49F8B4CC8493B22AE0F8D329EFA34205599E1138E57D33302B8A7B76F085DED053530B0F79D0DC71E257C99D80D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cmrinsure-my.sharepoint.com/ScriptResource.axd?d=cIUfeLIIIpVJe0ra_eq80vJ2bC2Z2x5DSGiyl1HHlOpLsB3TbT7B_amVBaprUbr7J_tcdrfO71le-AtUnKFdU7zkoUcfSAypCyNz6IB3qClq6mHDKv8dxmiFOOgOH9LBJtHObekBtvUH3pz9IlvA5PJLgbeYcDB9so3475Nrsl41&t=58ba508e
Preview:	.var Page_ValidationVer = "125";..var Page_IsValid = true;..var Page_BlockSubmit = false;..var Page_InvalidControlToBeFocused = null;..var Page_TextTypes = /^(text|password|file|search|tel|url|email|number|range|color|datetime|date|month|week|time|datetime-local)$/i;..function ValidatorUpdateDisplay(val) {.. if (typeof(val.display) == "string") {.. if (val.display == "None") {.. return;.. }.. if (val.display == "Dynamic") {.. val.style.display = val.isvalid ? "none" : "inline";.. return;.. }.. }.. if ((navigator.userAgent.indexOf("Mac") > -1) &&.. (navigator.userAgent.indexOf("MSIE") > -1)) {.. val.style.display = "inline";.. }.. val.style.visibility = val.isvalid ? "hidden" : "visible";..}..function ValidatorUpdateIsValid() {.. Page_IsValid = AllValidatorsValid(Page_Validators);..}..function AllValidatorsValid(validators) {.. if ((typeof(validators) != "undefined") && (validators != null)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Home_HMC_HighlightFeature_Fall_20_8_V1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1920x720, frames 3
Category:	downloaded
Size (bytes):	94011
Entropy (8bit):	7.761835215753565
Encrypted:	false
SSDEEP:	1536:2WZZOWshomizPQV3HQ5KnA5h5b4qaHudQg93P7tp+B+FBJ2R3XPqPrcjSqexa:p2WFvzPO3w5KnAj5PaOdFZpkiBoR/qPo
MD5:	4A919E00A7A8332C8294EE595A581378
SHA1:	1993BEDD791AEE3D97F2669E248E4FE81AE4C13E
SHA-256:	1B5788B11341A96171ABE3F04B6486D10BBBB833D704D1AF78900845F9529A2F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Home_HMC_HighlightFeature_Fall_20_8_V1[1].jpg	
SHA-512:	C4E3DDB8141923D60D442E3EE50C52183727C6B0955E15E350C66FA431E3A1A1E8DEC8AF34E3DB8AA99E2A2336F252FB5DE9970284E26E5550A9D5E8B23A1C2D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Surface_Home_HMC_HighlightFeature_Fall_20_8_V1.jpg?version=f7aa0cde-6334-bff7-e891-209770c7c9de
Preview:	......JFIF..... .....v.....^>.B.....O6./c.....E.O.....}.....c...wf...v.....K.Z. 'L.U..g. .....H.....".w.....$qW.....T.N"./.}..@.....q.....QS;.b.(.....|.|.g.y.ys.P.....?.<G... {GQ>.lh....9s..`.....K.?..S.6.{6|...).z....O.h.....{.3....N.:|.Q..K./..S`.....n_...(..:o.G....C.n>.....oz.Q..sf.:(...b..>z.....(..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Home_Hero_20_mosaic_Book3_SingleTile_V1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 950x1072, frames 3
Category:	downloaded
Size (bytes):	47546
Entropy (8bit):	7.560178599093037
Encrypted:	false
SSDEEP:	768:LirBYPRQ0yVPKp4FTlRjWnpFNZNDTULkH7QXJgjCLQjT+8/4dxc/SZ+E7Jljo2Xs:LirBcC0yNY4Fj2zBekbQXJlWqKbES+Gi
MD5:	D6B0CA518014F666D181B0BAF1E380C8
SHA1:	7CF748BD54B8C74D3230DCCCDFA6D299AD33B41D
SHA-256:	EA9D5487D96A57512479D6E566DB1C7B1760533C82B94CE4AA9D9A78DCE232B0
SHA-512:	55EA772AF03BF1EA302CA7E7CC625FFF49B3837CE6709C6F9A4C87E0823C4D38ACE93248F517E1F1AB2D9B94F90850748494E210E77D11BF8CC947EFA563931
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Surface_Home_Hero_20_mosaic_Book3_SingleTile_V1.jpg?version=f7a8f28a-7d43-8b2a-35e2-b9fca7693a53
Preview:	......JFIF.....0..... .....6q5zM..E.{[e.....1.>.S...t.]&.G..it.m&...V=..CG.....?%.E.V..j.....,b.>..... .....)...-.j.6m....b.....Oj.@.....o.dddd..eeee.f.gfd\G.....9...n...M1.....V.....&.-.M.....?.yG.y.....)..).""....Z.{.Y .....:..v.E4E4....S|....>..... .....i....E1.....O....M.)..i.b!.....jo.....z(..i..b...!..7.{.=. .....G..).i.." ..<....z.....|..9.i.)..i.b"!.|...W.;$.....v...".b...B*.?.....t?O{.....""".B.k.K..l..... .....g.)DE0.E1.C.s..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Home_Mosic_Fall_20_Duo_en-us_V1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 950x1072, frames 3
Category:	downloaded
Size (bytes):	102091
Entropy (8bit):	7.87868298982907
Encrypted:	false
SSDEEP:	3072:+/ka6vkDIAa8Ee7FX0aDiyBOc3+Rk8WUSy0CL2:+hvVjYlynr8WzLCL2
MD5:	6B8C057D7AB2812E9B15DA94A989CA37
SHA1:	82B0BFB278B118B1870881ED1B93D2E9B6F0F1D9
SHA-256:	527B5E7083E67760C3BA0CD6916781BCF4ED63FC9030A822EDB574DC2CA0CB49
SHA-512:	1AA84D4047A5F504A8F1D0C14AD2102A012748A37AF9AF8406DEDF19C4D251B0FF9EDBB661703FB0D89CED27B7DBA3ED8001E10650CE7B55B032DF33508C22C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Surface_Home_Mosic_Fall_20_Duo_en-us_V1.png?version=affd3171-0839-a6bc-6e2e-5e26d0093b63
Preview:	......JFIF.....0.....%H.....*.....U ....T.....UR.....@.....UH.....*.....X.....cD.....*.....UR.....@.....UH.....*.... .....X.....cD.....*.....U..... .....V4@.....h.....X.....cD.....*.....U..... ....V4@.....h.....X.....cD.....*.....U..... .....V4@.....h.....X.....cD.....*..... UR.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Home_Mosic_Fall_20_EarBuds_en-us_V1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 474x535, frames 3
Category:	downloaded
Size (bytes):	17680
Entropy (8bit):	7.79542847424389
Encrypted:	false
SSDEEP:	384:f3LF5iwyxwLm+LlXDLASSSSSSSS9YocA+kh25s2QehVr9g4dzAClY8q:Z5iwyxibtDLjkh25s1eh0qzAC28q
MD5:	469697DB09AF04FB5A5398A39FB2F9C0
SHA1:	B86CB15A1CDF51492DDAC895B330F51AC7CF032E
SHA-256:	EFAEC56D85C230E0D0960E4034940AB2CA04E12E4C184CE62FA0009A09DA0302
SHA-512:	EBEC36DCF6E40B7218FCC53F5C8F8E19C5EA159D63D88B489A965C0817C231522DB8C5EC50F2B00D123726F61BCAD61B843BF4866ABF9E4DDEBAD35C8FE5475

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Home_Mosic_Fall_20_EarBuds_en-us_V1[1].png	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Surface_Home_Mosic_Fall_20_EarBuds_en-us_V1.png?version=6b93a52b-8e56-b9f3-e353-0f0a4761d3c2
Preview:	......JFIF.....<.+ ....5.......?.`W4.....N....B$.....M..^.V.....Z..O.~._..s...M.....<{..n.t...oE.....#..f.....0.....OMS...?...v.....e....>+.Q_..6.1.:./....j|.SVoI.....|%...y.6.w...l.\..9....v. .....{;/=.f.....@.|.....<.A..3.....Z}Q....v....{.H.....+9.~.g.....?5.w..]vR.{.....e.....z.....[.....|..e.U.....Q.....>.....J..U..3.U2..\.....>...[.*.}'.\.s.?.@.....K .6.1.....G.k|..v.g{....a.....|.6..8^.....+.;.]....k<...)L....U.....|u...U~.%).DD&.....0...{...S3$E4Z....-....?.^.....;m.c....+.I.N.!..TN.1....v...xg..... .9....~7..9k...yX..G.....&S..C.$.G'...8..._H..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Home_Mosic_Fall_20_Go_2_en-us_V1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 950x1072, frames 3
Category:	downloaded
Size (bytes):	77480
Entropy (8bit):	7.823491143728619
Encrypted:	false
SSDEEP:	1536:XIx6333eryHRVkrRhOHq0nKZ26C1q3p7DwkQgFGZwsTGVAifVXj:XI4333e8Vkv0nPbUvFQ3yyurT
MD5:	FBED9D481231EBB984FE541BDA574255
SHA1:	1F99B347A7FBE31303E38731BF7C3F160459A91F
SHA-256:	C10CCAC2279EEB7A44DD9BEBC9543F94F5147B07E2CBF23466952A7BC85B150C
SHA-512:	2CABD964C71C8F288662A4B0B9EC9480E2D0555EA03955E44B01E6996AAC67D29F81DFBD4C25AF4D6C05A74A6910644812618A8A120D3F6BF57991F7A2903B2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Surface_Home_Mosic_Fall_20_Go_2_en-us_V1.jpg?version=45fd9288-3840-0d86-599c-77989e84ed43
Preview:	......JFIF.....0..... .....?....5ID...@...k._X.`.....G....j.....`.....'.+.`....p.....Nv`.....'....~.....z...._..."&@.....7.'.....p....o... :7.?C{Fk.....O....k..... ..y....r@|.._t.+.. .....'.k.o.?.....\..g..`#...;....r.....'.k.o.?.....|..g..`+..\..}.. .....Y....p.....:..'3.Y...X....=..l.2.....#.b.....~..;....7.....9.....'.....'.....u..|...Nz....:s.av.C .....@... ."......g.'.....p+.....r.....O...~...X.b.X.....?.r~..9.W..=y...;g!.....Z.b...DDU.....:..VO.....W."..gl.2.....7.....Z.b+...DB..@....U....c..~x.,?Vv.C .....?....+.....DV"....A..(.T.%.. u..d..<y...;g!.....!.DDD""!..D".A.u/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Home_Mosic_Fall_20_HeadPhones_2_en-us_V1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 445x510, frames 3
Category:	downloaded
Size (bytes):	21795
Entropy (8bit):	7.827529962147998
Encrypted:	false
SSDEEP:	384:fAhpfvsieRUHdlFxiJ9/EfcwZF5UPwr4IvVnjtx+8dbMuOGP9VBbUblZ5TnO:wIRUHHqJ9cfcwfQIvVjt06AA9VBbUZZO
MD5:	E2B7EDC672216BC2FEFFC63F31488B6B
SHA1:	D478F3A4A7A42D7903EA6F62727568B009E15B11
SHA-256:	65528CCD825EA77243F6FCED7FB48EC90E3828973374E2BC594A48E13F424426
SHA-512:	195B9323F0BF72B3FB4048674679A9141533A327B0B52EDEA612A661DDD02B2AF7F04A799DB3FA5083D395F7AC84AA0962A025AE9A97E65D72D2AA86B9908DD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Surface_Home_Mosic_Fall_20_HeadPhones_2_en-us_V1.png?version=892ac247-97ae-9d01-c3c1-265438fa3541
Preview:	......JFIF.....4...8..%.....W.e;....._Go. .....M ...c.....=.....!-a.^m.[w..`.....,...._..F.d.*.....(t...2N..m&...X.....kd..g.y*..F..m.....GZ..f]|o]..+..[.0.....Y....7...<w..1.>..@....tj.uy.e7.5.....{.....5...lx.u.E..8..U..P.....:..p.,.y&u u.5.).....[.;...v.9C..]W.28.....H#.K...dW,J.....W.K.W.f..e..>[=.. .....{nA.f9.....A...Y...T.....RH.....Bz.Wn.%^2...g.k/.....".Q.e..{uFe.QP.....C....(.....A.....`..ln. .....q..|.....L...s(.....!.k.(.u.*./wOF6`.....S.....u..l.....E.?~o.zp.....:[].....6...N...}A.@....k...2..]f..f.....=.....d.....yM..vd.....(...-...h.?go..0....".-...ro`.<w.vo~.....Q.....b .....x..KW.....,.....:un.z+..<....n.....D.....=...../.....Ms..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Home_Mosic_Fall_20_LaptopG_en-us_V1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 950x1072, frames 3
Category:	downloaded
Size (bytes):	48525
Entropy (8bit):	7.6457372108718
Encrypted:	false
SSDEEP:	768:1nD6lwK+7n9loEGM7zfIfyFax+/FL6AyMsmU5cv20KMNnh/H57/QIdKHfJar8TOo:mwdZ21M7kKFaxWuxm2cvdjJhxPsHBxao
MD5:	01E9300F5E6CDA7FE82E68FDFE4D5EE4
SHA1:	237CEA685592BE046F4452BF5B3C7296D98E0602
SHA-256:	C53B053590E873739D887514453FDE4459239FC805B93CAAC19BDA7511C6F28D
SHA-512:	B5CD46EEBA5F75EB3C77E54A2158411EC86BBFD1894132C79FB51316AF555906F454C305BDBEF3E1AC5D548A78CC84303C229A40CCE4BD2424914A3A3DE789 3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Home_Mosic_Fall_20_LaptopG_en-us_V1[1].jpg	
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Surface_Home_Mosic_Fall_20_LaptopG_en-us_V1.jpg?version=2d178933-8079-1585-f38e-4215399226b2
Preview:	......JFIF.....0..... .....g.iJ.+.L.....J..)L.).y .36....o.....+JR..:gL..:g.y.y.T.#.n.....)J.:R...L...L..2.yS<.....y..)JR...:g.y.*e.3.<..<..s.....c.kJR..:S<.3.<.3.*g.y.<.....aj.:.:R..<.L..y.3.<.y.G.<.....).).3 .y.L..:g.y.<.3.....R..)L.Jg.3.y.L.t..3.t.?q.....G...i.).3.y.:g.3.y.L.t..._F.....g.u.3.3.t.y.L.t.:gL.L.J}_.`.....?.*.J.L.L.t..<.3.t.t.(.....f..t.).3.3..:gL.L.)JR..'. .....t.t.3.t..: S:S:gJR..+.a.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Home_Mosic_Fall_20_Laptop_3_en-us_V1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 950x1072, frames 3
Category:	downloaded
Size (bytes):	159894
Entropy (8bit):	7.945085398678266
Encrypted:	false
SSDEEP:	3072:9ixucgsrBaIGZ89WEEJzDNvITTnxczsG5YGxDmIJFm/cZCLA0A2HUH9L0EgU:5eaIGZfINvInxczsVQDxhp0N0J
MD5:	860B8CA3863D541D7FBD1C9222E8D4D8
SHA1:	0B385AA2FF759C2E4C480ED5DCBB9A55BEB1E89A
SHA-256:	1DFB72F21C4D51B0BE6F3A2A5FE86C2F3A2FDFBB8A52AFC934F5089B5C4AE755
SHA-512:	56BAB47DE59B5F563989C8B3B0B4FE0603A7553B69B420667E8FF94EB638B51989E2D85ADD400A4DBD1E686D00E9140C2556A32E1BF3B2601DBAA6CD6A6E77A 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Surface_Home_Mosic_Fall_20_Laptop_3_en-us_V1.png?version=22b99f03-0a8b-056a-facb-86db76b6765b
Preview:	......JFIF.....0.....44.....4..1.@.....4. @4.....@.....4.....0M.CQ.....hi.....b.h..C.....hb`..!.b....`..C@.4....@.....&....@..40.4..N.....1..@.0....@4...&&....4.44.M4..D.....h.....hhi...41.@.... ...hi..X..`..h.....i.....@..... . ..0..0.h.h.h...h.....!....`.....L...`.....4....`..M4...@....4...0..U.....M.@..44..Q..Q.....P.2$@M]..A... `...+....I....CC@.'...)0..1.....Z.1...4....`.....4....&.....L$.9.#...@.4....&..... .`.4.4...i....LI(..".....&H..e..0.4.@.b..l`.....h...RR .(D.bEL$.....?`hh....4.@1...0.....@...]3b.Q..c..b..!.<..;.bhi..C@.X..@.0.4...}.NCBHM.....%7.).r.R$H..i.0.@...CP..1....M...../. ..k.F.....M.'|...:..q..d..7)...{.`.....&.Z...0....?.h..H.t.e..(...?RQ~.)W..V&.I.|..{..... .....i..'.zaTj.....0....._

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Home_Mosic_Fall_20_Studio_2_en-us_V1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 950x1072, frames 3
Category:	downloaded
Size (bytes):	56357
Entropy (8bit):	7.699747906583858
Encrypted:	false
SSDEEP:	768:sTdzEAUTw19JQTgD3hrgwapzDbAv6g8soD3SR0FvDW9m+XeTbFAjHjr5JJZoSAXv:lqwGTgD3YoKserW99utQHLMlXnuS
MD5:	E9CEC502203B2E9DFE795AA195389DAF
SHA1:	09613D6F8E73DC6FCE827810EA86DEA1BA78DA89
SHA-256:	C892F89AB3169BFDF0337C9A14305FFEDAD978E7D0840500A338F929C70D3187
SHA-512:	B307133786B53D858860622595B18E08FDC21AF7EE8C515F9A67B1B7219215C8CA8C11A6E5411BC9AB859FCA1E069C3C92D34E3B9E229F85BBE5CDA51FCB35E B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Surface_Home_Mosic_Fall_20_Studio_2_en-us_V1.jpg?version=b13db182-9214-d5a4-1a51-2ee8aedb503a
Preview:	......JFIF.....0.....4..... .....p"@.BPJ%..`....o.sl.....'H&.....I.....y..J.....A!.....{w..0.....E... LH"H$.....y..N.z.....ZH&...J.....P..D.a$HD.1>f.....<../m....&.....P.L&...(.../3:..P.....?.....D&..0.&....a0&.A0.&&..y....z.....b%.P.$.0H..L&..0.A0%.f.....<~.7m.. ..$J$!"..P..%."bbHJ....a.'..L.....Q.m.0LLL..`L&.%.@..bb`...a....@....<}.Gm}.....11".a0.L...J%....a.....<\|.Gm...(L....10....L..D.a.oX.`.....:..oF%....L.@.....$..D.0..f....`. O.....d....&..I.L...0&...3:..._.....x...z8....H.... ."D$..fu...a?A.....=..z!... .....3.?.{.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Home_Mosic_Fall_20_prox_en-us_V1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 950x1072, frames 3
Category:	downloaded
Size (bytes):	54246
Entropy (8bit):	7.706147464132557
Encrypted:	false
SSDEEP:	768:FaHBCUPlrPHyFrZ9Ji7qkgooBD280aF/1lXiKt9iF7BjVlad2klUThozfzOP3Voh:Fa/FPHyFrZqQ/qyKfiF1RJ27BY32RVio
MD5:	5D67E6565EA5DC9515BEABC01B0CF8C8
SHA1:	B6577F62AE29BE1E7E0D640BBEFD3E7062B628C2
SHA-256:	0087B5D0BAB39C5CB9634841C44D1556189FBB3782222E1D174AFF16A8C43C47
SHA-512:	91F98F53DB1B8F5162EBE6A35AFD821C4280080E578ED6BE23057C58620386A7DFF8A7DA6F6C76C36658E2662EDFF257768CAF710B0F18F414F703BDF84DEE7(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Surface_Home_Mosic_Fall_20_prox_en-us_V1.jpg?version=ff429f4d-7a62-77bc-52e7-8526e5c4245a

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Home_Mosic_Fall_20_prox_en-us_V1[1].jpg	
Preview:	......JFIF.....0..... .....5~'.....<+.-z.....7./.....\.....5 }..w.....9_.m.....-...ie..X.....Gc...vU/.].].g.....}3.....e....j.kL.:.....>@.....s..m...p.u.]O.....k...>..Q.f7r.....1|.c.=.ddddd...P.....>..>.Vq.9.....9.+..x.C{'###".- .t@..5.8y_?.....HR.....S..{.7.f....w.....[=.....j.)L.M@....#...0..k.?<..rrr22o...L...O.\../.}....k=^.XF..i;.....F.....t.z ..[..s|.....{.....6{.T...{..m.....n..R..[.P.KP.j..D!Y. ....c..c.....w.....GO...mz]..bk

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Lg_Generic_ContentPlacement_3UP_20_Acc_V1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 485x273, frames 3
Category:	downloaded
Size (bytes):	30728
Entropy (8bit):	7.953210799904295
Encrypted:	false
SSDEEP:	768:KrDxTq/2nVE2T/Jq4J233XRnFyvh89kjLR6E2yfN:IxTKyVES/JMuvh89koGN
MD5:	3C20EE98F647F4F59C1EB22EF1419FAA
SHA1:	C23700733C7CCC6DFF940A44C94670F0E7CBCD29
SHA-256:	E671FB08F0A3F04D8987F207A7F4461F49FE28A953A607D956F870C7847E7A69
SHA-512:	09F6230F5A732742B49CCA67696DDD6E47C40F54BB700E221A6414E3839B740CB7D3DEC9EED174098A8BEDE05ED6CA44FBCF383DA8ED435581A2308DD265311
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Surface_Lg_Generic_ContentPlacement_3UP_20_Acc_V1.jpg?version=0a81779c-5c7e-a61b-908c-4ce93f2a6950
Preview:	......JFIF.....n.....1..knJ9s0.+y..''V=..*.... u''.....<...l..w...'!U).qW.q..7^...Z-y.s@.....)A.:M..k'.W..''..).$.J....z.....@.....x...@.3.e.\.u...h.(..O.,.....R../.x....5..*M.8.T.x.2.b...''..Vz..... .<..=...-/E]...S .tR\K"1.....J.8./C..@ ..Q .....-../?..Y&.....Ub..&VU.~..wh.@....b.G.x.....}.}..&....$.=.....6...#yU.....NZ...L+._G:k.7.....~..J.....s..^EU....9....p...m....6..3.;.U...M.J.....B2.(....). .|?h.....O;Y....E....J.B.G. .V..L?.....<..H.l...._....x...O9M.V.~.\.u.z3.UP.#5&%..lu~V....U.l....N....K...K...V..0T..n..9ESW.G..4.1....6.Mfw...NM.a.....n?.tu/P.....:..<..r..5...b3....F'..?..}...W....~.a.#...~@...G.. .kZ[R..?I.n..h..[.....=.....P.[.j.W.7.i*..?...d..f.N.....iuHX....}u..+]....4...^..b_X.....,GN.=...'.....sb..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Surface_Lg_Generic_ContentPlacement_3UP_20_Business_V1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 485x272, frames 3
Category:	downloaded
Size (bytes):	41566
Entropy (8bit):	7.970894420395129
Encrypted:	false
SSDEEP:	768:NlU3wgCeWy4Z3TUYX6jXN1NXzXoYauAGNcNtnLTn0U0S1qUPgIIIEg:Nl4wgC/y4ZxXaFzFauHN4RvnH0fVg
MD5:	60890C74D58E525DDDA8DB3EB2486C94
SHA1:	88285C36DC67349F4CD1460EABA9F565D9B7E575
SHA-256:	6BA51FEA14178DCF16DD545430BCB66C9AC889C4C670EB4D5F9F09C57A0F373D
SHA-512:	9CB5E7F4F920AA0C4DF6BE1646ECE722462C7F3A18BB736EDFD00BB9E135C5424E983D77111920FA8433CA3C6F3339DE50EE5E0EA930B3B16B7E3812EC6618A4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Surface_Lg_Generic_ContentPlacement_3UP_20_Business_V1.jpg?version=89c8b139-8e32-4d1f-6dd9-09b13aeb5afe
Preview:	......Exif..II*.....Ducky.....P.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 6.0-c002 79.164352, 2020/01/30-15:50:38 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:7E6E3AA4917511EA96B8F13B1A010E1A" xmpMM:InstanceID="xmp.iid:12627EF0916C11EA96B8F13B1A010E1A" xmp:CreatorTool="Adobe Photoshop 2020 Macintosh"> <xmpMM:DerivedFrom stRef:instanceID="A3345D466467131E4C37D35A8DE426A4" stRef:documentID="A3345D466467131E4C37D35A8DE426A4"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\amx.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	67346
Entropy (8bit):	4.973528323066423
Encrypted:	false
SSDEEP:	384:g6vaxTeTqydNWdU++Pfz5KnlgWSWNa+EyHY4ArMivOVkdrV2448Hj2VGfF:3MfyHCOP3+D8MIAWxF
MD5:	25414FA5E70EBD15D18B57E095000EF0
SHA1:	87D91E4B2D30D0D6FFAA5C66FDDEBA7D2E00BAC1
SHA-256:	AB582F024CB8904F3B6C0D9D5560AEAFB1B6A108A4F95605DA6CB85D775BBAD9
SHA-512:	C468A14C617B207CECB3E36574BC50EC0CDC8716886824F5F9ABA2CAADCAA0C08BF356041BE5B493A61E28AD11B091670531BA4439DFEB7FA5EEA5E19237A6E5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\amx.min[1].css	
IE Cache URL:	http://https://account.microsoft.com/dist/oneui.razor/public/styles/amx.min.css?v=AB582F024CB8904F3B6C0D9D5560AEAFB1B6A108A4F95605DA6CB85D775BBAD9
Preview:	.mee-error-text{color:#d02e00}.mee-success-text{color:#107C10}.x-screen-reader{position:absolute!important;overflow:hidden!important;clip:rect(1px,1px,1px,1px)!important;width:1px!important;height:1px!important;border:none!important;padding:0!important;margin:0!important}.@font-face{font-family:'Membership Icons';src:url(../../../../Styles/Fonts/MemMDL2.eot);src:url(../../../../Styles/Fonts/MemMDL2.eot?#iefix) format('embedded-opentype'),url(../../../../Styles/Fonts/MemMDL2.woff2) format('woff2'),url(../../../../Styles/Fonts/MemMDL2.woff) format('woff'),url(../../../../Styles/Fonts/MemMDL2.ttf) format('truetype'),url('../Fonts/MemMDL2.svg#Membership Icons') format('svg')}.mee-icon{position:relative;top:1px;display:inline-block;font-family:'Membership Icons';font-style:normal;font-weight:400;line-height:1;-webkit-font-smoothing:antialiased}.mee-icon-GlobalNavButton:before{content:"\E700"}.mee-icon-Wifi:before{content:"\E701"}.mee-icon-Bluetooth:before{content:"\E702"}.mee-icon-Connect:b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\c9-860587[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	328433
Entropy (8bit):	5.2967835820513045
Encrypted:	false
SSDEEP:	6144:xAuXzUqR1sJj0qRORPvksdmXca3p8q9Yq2j:xvzU1j4Ma
MD5:	0F91FD60790BAC7B37B864888854F473
SHA1:	7A5671EF91D52617588C16B5A6B6E87371E200CE
SHA-256:	9A0512A21E8F4F28378EF3A982FCEDF57B7DF56E45A5B00B034FED10C8A3DF06
SHA-512:	D1FF6FE92C8013A2DEAEF5095E8ED7F751CC5F6896841E8B7FDE5AE48BA01A37BC599C4BBBD42F1C1BC5472BB02A2B2B99B5F3F5BE81D84C03000BF9196154C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/mscomhp/_scrf/js/themes=default/e1-a50eee/e7-954872/77-04a268/11-240c7b/5c-0bb0c0/81-a5a694/2f-63ce8f/6a-f6eed8/dc-7e9864/4f-5115f8/7d-266f10/4a-abd94b/ab-b04110/fd-7cc407/a4-fd2a9b/7b-131f20/66-c19a96/d0-633018/74-b70f5f/84-e0fd46/10-434ba8/8a-fde610/80-c05e42/a5-ef9ca1/f8-6a3735/b8-96db64/b4-d9c6d1/59-aa2448/d5-2b21b0/c5-346220/d6-6bf74f/10-1c7804/b8-527d75/57-0776c0/7a-fdafe7/18-91dd3c/88-3094ff/bf-4fabe5/36-b9cc25/12-fd63db/85-b1c94b/6a-582442/64-02965a/37-f22d3d/33-eb67f7/fb-890cea/c9-860587?ver=2.0
Preview:	define("componentFactory",["require","exports","htmlExtensions","utility","stringExtensions"],function(n,t,i,r,u){"use strict";Object.defineProperty(t,"__esModule",{value:!0});var f=function(){function n(){}return n.create=function(t){for(var i,r=0,u=t;r<u.length;r++){if(i=u[r],!i.c&&!i.component)throw"factoryInput should has either component or c to tell the factory what component to create.Eg.ComponentFactory.create([{ c: Carousel] or ComponentFactory.create([component: Carousel])";n.createComponent(i.component||i.c,i)}},n.createComponent=function(t,r){if(t){var o=r&&r.eventToBind?r.eventToBind:"",f=r&&r.selector?r.selector:t.selector,s=r&&r.context?r.context:null,u=[],e=function(n,f,e){var a,c,l,o,h;for(a=r.elements?r.elements:f?i.selectElementsT(f,s):[document.body],c=0,l=a;c<l.length;c++)o=l[c],o.mwfInstances||(o.mwfInstances={}),o.mwfInstances[n]?u.push(o.mwfInstances[n]):(h=new t(o,e),(!h.isObserving||h.isObserving())&&(o.mwfInstances[n]=h,u.push(h)))};switch(o){case"DOMContent

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\cartcount[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2566
Entropy (8bit):	4.393500974386876
Encrypted:	false
SSDEEP:	24:KPv6HUY5+yAZFAXJqiXZXTMxPv6HUY5+yAZFAXJqiXZXTMK:EyHgyYFGMEZo9yHgyYFGMEZoK
MD5:	EB42BF181717EC1B1C4D9458A7AEA1C4
SHA1:	69FE74312A74D5D71FD4124F96D58D35AA1FFCFA
SHA-256:	8F6ABC9668C8AA27926673F6FD5118AFFCA717A124A565F96D4DE4143B96DFAB
SHA-512:	A73A12DCE699ED7E1F60EA6C6C097F68FB7397044A4E275C79A0206D3EA18986B606FD45E81E6704463827BC97A081352BEF59B79E3B5A024FD7C104F243C982
Malicious:	false
Reputation:	low
Preview:	.....<!DOCTYPE html>..<html>..<head>.. <title>title</title>..</head>..<body>.. <script>.. function getCartItemCountFromCookie() {.. var name = 'cartItemCount=';.. var allCookies = document.cookie.split(';');.. for (var i = 0; i < allCookies.length; i++) {.. var c = allCookies[i];.. while (c.charAt(0) === ' ') {.. c = c.substring(1);.. }.. if (c.indexOf(name) === 0) {.. return c.substring(name.length, c.length);.. }.. }.. return 0;.. }.... var count = getCartItemCountFromCookie();.... var parentHost = '';.. var parentOriginProtocol = '';.. var parentOrigin = '';.. try {.. parentHost = parent.location.hostname || '';.. parentOriginProtocol = parent.location.protocol;.. parentOrigin = parent.location.origin;.. } catch {..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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:OzCPZkTP3bDLH0tfRqQ0xtLfj4ZDSIpTt813viY8R1j35Ap7LQZLPPJH7PAbOCxR:clZAXLkeedh
MD5:	0DCFF2779D4542C11AD9C9C19DF8328D
SHA1:	D7EFAE8E66FA6B4C335826BFD8C56C6F142E4254
SHA-256:	440D8292ABDF80DD6E8A9D9FAEA83367CE57BD1A1A8D153EDC358DB5F97EFF35
SHA-512:	CC747AA36ADEE4CBA4236F01820CE9661214C649DCF23227D7CF9187E24F2D15DBA43E9B706B30DC3D55060E08601575EAB0256306AEA28F3544BAD4BC33E93

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\cf-7c36ab[1].css	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-wcus-prod/west-european/shell/_scrf/css/themes=default.device=uplevel_web_pc/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 P arty Code to you under the terms in which you received the Microsoft software or the services, unless Microsoft clearly states that such Microsoft terms do NOT apply for a particular Third Party Code. Unless applicable law gives you more rights, Microsoft reserves all other rights not expressly granted under such agreement(s), whether by implication, estoppel or otherwise.*/./*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */.body{margin:0}.context-uh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\cf-7c36ab[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	236261
Entropy (8bit):	5.071063191447717
Encrypted:	false
SSDEEP:	3072:wYzddg8HPbn/hL4fbv3DlF+EkyfJY6F0AJL55gGHjkzmfeT5NbORfJ4J0ZRV8+ug:aLkeeduZKRFG
MD5:	242E774D306438BAAF408B17A5E74E01
SHA1:	F523F1804CA4C542D58FBA4D133A5C3CC7027D58
SHA-256:	57059C202253CBCBF070E96129D93E1C3B8767A8A86B0A4025189A7E99BA5105
SHA-512:	2590153DF493BA93D994AA412BBC8C007A03AA3BDE83445EC0527FED57D538921BD70D7B18D9E8AC7EEB88EA1ECCC56BE632FD8825E27B983B2B09413FF24D21
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/west-european/MICROSOFT-365/_scrf/css/themes=default.device=uplevel_web_pc_ie/a7-5072ba/b1-63dc4a/88-fcf4b8/94-28a114/e5-1b8a4f/98-bd0547/96-b2fd92/b5-285959/a6-41cce0/21-7d6c87/c7-542157/c3-953460/60-1db702/a3-962591/bf-60f63e/81-8ca29e/c0-379397/fd-9178b9/cf-7c36ab?ver=2.0
Preview:	@charset "UTF-8";.x-hidden-none-mobile-vp{display:none !important}@media screen and (-ms-high-contrast:active){.c-uhfh button,.c-uhfh .glyph-shopping-cart,.c-me .msame_Header{border:none !important}.c-logo{margin-right:1px;border:none !important;outline:none !important}.c-logo.c-cat-logo:focus>span:before,.c-logo.c-cat-logo:hover>span:before{background:WindowText}.c-uhf-nav-link{border:none !important}.c-uhf-nav-link:hover{text-decoration:underline !important}#search{backgrou nd:Window;color:WindowText}#search span{vertical-align:top}.c-uhfh.c-sgl-stck .c-uhf-menu button:focus,.c-uhfh.c-sgl-stck .c-uhf-menu a:focus,.c-uhfh.c-sgl-stck .c-uhf-na v-link:focus,.c-uhfh.c-sgl-stck .c-logo.c-sgl-stk-uhfLogo:focus,.c-uhfh.c-sgl-stck .c-logo.c-cat-logo:focus,.c-uhfh.c-sgl-stck .c-search #search:focus,.c-uhfh.c-sgl-stck .glyph-shopping-cart:focus,.c-uhfh.c-sgl-stck .glyph-global-nav-button:focus,.c-uhfh.c-sgl-stck .glyph-shopping-bag:focus{outline:2px solid WindowText !important}.c-uhfh.c-sgl-stck

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=1460
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMo reInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\e0-e56761[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	29974
Entropy (8bit):	5.011040310993689
Encrypted:	false
SSDEEP:	768:68ErSqwYkllNQ4gYq0qM+iPAeUxUDUzUBGjjjFjtrVrzdrdq:68ErSqwYkzlNQ4gYq0qM+iPAeUxUDUzM

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\e0-e56761[1].css	
MD5:	DBA5433A4DAC62BA52560F26B09F68C9
SHA1:	6033C988880EA91E6122D7B7ACA28CC996293519
SHA-256:	103C8117C8EBB5ED431E32BE13F33AB9FA8B0E63D3CC0DB48E0593D31B57651B
SHA-512:	CF52047D412535585A79D325A67F8D695B2BF768A4CE564F617739DF201E4B75F54B7BFDD007EECB9EF1BEC97AA42EF0A15EE01D201E9F889AB5F707B86D5F96
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/west-european/mscomhp/_scrf/css/themes=default.device=uplevel_web_pc_ie/5a-0bf7d0/cd-a7831c/e0-e56761?ver=2.0
Preview:	.html,body,#primaryArea,#primaryR1,#videoplayeriframe{height:100%;width:100%;overflow:hidden}.m-video-player.full-width{padding-left:0;padding-right:0}.m-video-player.expand-preview-image .x-sfa-video img{width:100%;display:inline-block}.x-sfa-video{display:flex;height:100%;overflow:hidden;width:100%}.x-sfa-video img{height:100%;margin:auto;display:block}.x-sfa-video .f-video-trigger section div button{background:rgba(0,0,0,0.6) !important}.x-sfa-video:focus{outline:3px solid #FFF}.c-video-player{cursor:pointer}a.x-sfa-video .c-video-player{position:relative;padding-bottom:56.25% !important;padding-top:30px !important;height:0;overflow:hidden;min-width:320px}a.x-sfa-video .f-core-player{position:absolute;top:0;left:0;width:100%;height:100%}@media screen and (-ms-high-contrast: active){.c-video-player .f-video-trigger section{background:rgba(255,255,255,0)}}@media screen and (-ms-high-contrast: black-on-white){.c-video-player .f-video-trigger section{background:rgba(255,255,255,0)}}.c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\e3-082b89[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	110303
Entropy (8bit):	5.229738360351486
Encrypted:	false
SSDEEP:	1536:uzUHQTAz9ppxS7grUU59gQ9IwInL2dS6J09RhY8WOyd1EwgXA9GKaWAMKihAGDCD:uzUVppxvIeJ0y9d1EwgXA9JKinDCE54
MD5:	A6DC3EC8F98698CB7F93008BD6869649
SHA1:	51174DA1F2D44501B529CAE56ADB6D8F7C39B776
SHA-256:	A3A0C8FCBA47950DA4EB20467D4B24783F776FDBBB04287F2C45263A3DA8DB7F
SHA-512:	D992E264C8C2C4071B5DBA1E0AA622F4C55B9253C0771FF3296459E7DC67B1FD3BCBD7181A7DF51A8CEDDDB4CD1FEC966BFF1BEABF4FE1459E2409C4BE839E65
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/MICROSOFT-365/_scrf/js/themes=default/2f-63ce8f/2d-7a9063/dc-7e9864/4f-5115f8/7d-266f10/4a-abd94b/6d-c07ea1/29-1ec5a9/23-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;define("ajaxWithAnimation",["jqReady!","jsll"],function(n,t){var i=[" <\/span><\/span><\/span><\/span><\/span><\/div>"],u=function(t,r){var u=n(t),o,f,e;u.length&&(o=(r.loaderType||"").toUpperCase(),i[1]=o==="PROGRESS"||o==="PROGRESSBAR"?"regional":o==="SPINNERLARGE"?"local f-progress-large f-center":"local f-progress-small",r.margin&&r.margin.length&&(i[3]=r.margin),f=i.join(""),e=(r.loaderPosition||"").toUpperCase(),e==="TOP"||e==="BOTTOM"?(u.addClass("ajaxloader"),e==="BOTTOM"?u.append(f):u.prepend(f)):(u.parent().addClass("ajaxloader"),e==="BEFORE"?u.before(f):u.after(f)))},f=function(t,i){var r=n(t),u;r.length&&(u=(i.loaderPosition||"").toUpperCase(),u!=="TOP"&&u!=="BOTTOM"&&(r=r.parent()),r.removeClass("ajaxloader").children().remove(".c-progress"))},r=function(i){i.refreshElement&&u(i.refreshElement,i);var r=n.extend(i,{s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the website you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\facebook-gray[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\facebook-gray[1].svg	
Category:	downloaded
Size (bytes):	675
Entropy (8bit):	5.462138293900793
Encrypted:	false
SSDEEP:	12:TMHdPhGi/nzVcU3/KYf3nhJ3yNgJoHNWdtGe9SGUCl3L5ZaSNjeH4IEezK+:2dMATLf3G5kdtx9SGsL5ZEZEezK+
MD5:	F7BD2933A7854B8A43D3E3A04D65A184
SHA1:	8D809533E65ADC0B2478E615CAD0AE425A6C2A2B
SHA-256:	FE2A2C856A8E799BA099513E3A0E1CFF1FB6B2DD4A1EA520E26D1AB9F484CB4D
SHA-512:	EDA0D86B245E10819FD7351DE0B10FB6E6A13786F20F3B6001C5FA4003806F4A44FEA7660C94FC160030BECEC512A1EC06397C26344C24BD7497F0777E0350C3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/facebook-gray.svg?version=0b3295fd-6d09-d5a5-af3b-498b3ad72a95
Preview:	<?xml version="1.0" encoding="utf-8"?>. Generator: Adobe Illustrator 25.0.1, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->.<svg version="1.1" id="Bold" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px".. viewBox="0 0 150 150" style="enable-background:new 0 0 150 150;" xml:space="preserve">.<style type="text/css">...st0{fill:#FFFFFF;}...st1{fill:#232020;}.</style>.<rect x="0" class="st0" width="150" height="150"/>.<path class="st1" d="M100.7,24.9h13.7V1.1C112,0.7,103.9,0,94.4,0C74.7,0,61.2,12.4,61.2,35.2v21H39.4v26.7h21.8V150h26.7V82.9h20.9..l3.3-26.7H87.9V37.9C87.9,30.2,89.9,24.9,100.7,24.9L100.7,24.9z"/>.</svg>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery-1.11.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	95786
Entropy (8bit):	5.393689635062045
Encrypted:	false
SSDEEP:	1536:/PEkjP+iADIOr/NEe876nmBu3HvF38sEeLHFoqqhJ7SerN5wVl+xcBmPv7E+nzm6:ENMyqhJvN32cBC7M6Whca98HrB
MD5:	8101D596B2B8FA35FE3A634EA342D7C3
SHA1:	D6C1F41972DE07B09BFA63D2E50F9AB41EC372BD
SHA-256:	540BC6DEC1DD4B92EA4D3FB903F69EABF6D919AFD48F4E312B163C28CFF0F441
SHA-512:	9E1634EB02AB6ACDFD95BF6544EEFA278DFDEC21F55E94522DF2C949FB537A8DFEAB6BCFECF69E6C82C7F53A87F864699CE85F0068EE60C56655339927EEBC DB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.1.min.js
Preview:	/*! jQuery v1.11.1 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k={},l="1.11.1",m=function(a,b){return new m.fn.init(a,b)},n=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,o=/^-ms-/,p=/-([\da-z])/gi,q=function(a,b){return b.toUpperCase()};m.fn=m.prototype={jquery:l,constructor:m,selector:"",length:0,toArray:function(){return d.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var b=m.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a,b){return m.each(this,a,b)},map:function(a){return this.pushStack(m.map(this,function(b,c){ret

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\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:I6ibzTDpOGuAJ63YB9eSzDtQEspfAzyNyuBmOfAJYCM:/iPMYJ4GEAZoTyglcM
MD5:	CAD76E4816AF6890C9BFD02A6D1EA899
SHA1:	9EDC91541C31034FCE0D83AABBAAD4C314CD3D33
SHA-256:	D5794223D1A062E5DBE6C34C1994C8CE3792B24AFD5218D0644CB1F53DA4BE58
SHA-512:	24983A5856C2B4D8CBE2A4BD233A93B266A03D4218942E1D1733B33B65AB7A504AF0AC31DE2F1E69F6FF8CCD7A169CD4555539D34FFF8DE4CB8C98DB2DB2C 63
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.l.a.r.....V.e.r.s.i.o.n. .5...3.2.....S.e.g.o.e. .U.I.....RV.z..;~.....U.D.-..iu...N4P\..GLFM .Y.?.;..-...~~....Ox.M..".$.._.....g..sC*2..4W.....9AGc.[a..*.rCl,..@..U_..L...e..Ru.J.-.f..3.....S`.A.....K<;...n.Y...rli.....([...W...5k.....^K.G...U.@....2H..B.)N0w.....C..9..... ....#.l2,4..6y.3$b....K.wx...l.$E..?3.8.c...,x..t.wa.O....4.c...!..+.<EM...2T.>\..]4.A.H.;..G.....W.:.?...Z".....e....8....84.L,.)0..y.Xdd.Pa.@.&.o(.I.q.yF...[.y.m(D...(....T.....,A.;q.... .w.$..C..a.. .Y.O?{..0...'1.;C.,.....W..Q-..'.5tD@9..U...E4e.&_...S.Y...\)b.s.rIR.....%..R..KU O..{.0(.....^Q\^!.et...Kf%..K...}.1...S.{.....3p..]...|Y...w..|JeS$..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..\."..M

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\latest[2].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Segoe UI Light family

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\latest[2].eot	
Category:	downloaded
Size (bytes):	28315
Entropy (8bit):	7.9724193003797
Encrypted:	false
SSDEEP:	384:+R0Z7+bHAtrQ1yBFbgqLct7rJhhPLLkHsrvSzaJu4ml3n5o+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.l.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..66.....U.D.-..iu...4P\..GLFM..C?.;..-...~|...P..\.(..)RI.....>.>..CE..SsV.jPR...H.....].R..&.n.hT.....x.....q .....wA[....F.....c."....Zed..>.?...`..3...B..W....R....F.j....v..'?.5.k^.....+..a...)..._].x.#QSi.....|<t....k.;..Hv1.G...L$.9....5.t.:...V.Y.....\|.@....B.....P`..2.Z.0....2`.FR.MF8.x....GP0..$:.....PYm.22..."S."1.*j[=.=.mR.*.....j....&.4...k..].1@..y$....."y..C..g7..k.B*...V..F\...G.m.jK ...O....b.Qlo...!.N.V....t.[..p.N..~@1d...YX.."....R_i.4.$j.P..U....u9...<..6..4%.....9`.....S...N.Y..L..B$2\.E.vhe...n..h..5..Z..K?.H..S...2..=R..x.....EX.2.....$."....It8..z.+.h ..$.2*T....}Z../....p..b0ae.qq.(-v1..E.!.l".a..p.).:,.8t..7..^..W...4A.D\eOb$.....b.NI.Pe.#$.O38....,....g..&|...B{...].....9..u.8..~Y...3.X..ff.,.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\latest[3].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Segoe UI Semibold family
Category:	downloaded
Size (bytes):	30643
Entropy (8bit):	7.976822258863597
Encrypted:	false
SSDEEP:	768:UOtV1asJ9G0dAdnVrKX/HkVJRPvkgxYZ4Zoe:bLasJ9G0u0fk/RnkgxGof
MD5:	E812BA8B7E2A657F2B70CFACE93C7682
SHA1:	2F02CDDBB483F9B11BBBE74C3CA917A4C345FBAD
SHA-256:	3330C1DEAC468874238DD0C6BF902179A8731EDA8A208C7D01DAC0AB1EAE1BC9
SHA-512:	354B2DB12BC1D67F26F94352B0B663DAD64C46C107454FC19CFEA01C54BB09340BC26C06DE1B96FF826F5287CE246A6317722BAE41B72B63BA86FDAF844BA94E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://i.s-microsoft.com/fonts/segoe-ui/west-european/semibold/latest.eot?
Preview:	.w...v.....X.....LP#...B..... .....".S.e.g.o.e. .U.I. .S.e.m.i.b.o.l.d.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .5...3.2...".S.e.g.o.e. .U.I. .S.e.m.i.b.o.l.d.....H.P..lb.7^.....U.D.-..iu...:4P\..GLFM.Y.#?.;..-...~}_).z{.rmD.1".$....{.t....=...!cK...%.~.....g.....j.9S....6. ..n..V.]pz...e.....#X...=,.p.F..6&.VR...k$~J..n....7.....K.8..T.....x..J.....#.J.XaQ.Q%_{3..xr.... 0Dm...k..Ep.....>..?Pk!KB..C...Q.q..1=6<,.S.F.&B..J.....ya2b."S.....6.2.....H.....*..09A...Tb/.&.d..#.E.:.E.(..I5.M..444d.1.....K..I...I.O..VBb....:..:b..Mh.'=4.d/..o.k.mMm.....bx..!..S.@E.....>@:..k.JCas..7."..uG3hR.h..w..8W>.4.....pX....J..a....}.Y.....(>H^=.`=.mg*.!.....w'...J.<.ob..3A .../.....5%.'....XS0a.....I.Ia....a...=..g.....{V1+..".._)7$2 O..!bb.=..|.s.1..2qm..#.O.....+E(I..1....EgQ.....E)R.m.?.8.q...J.G.@!f..n.F.r#..(..2p.?.9.8..?.d]..s..0.9.f..A...r.iq....x.g.aO....S.....R0i..BT.yl.".<k...:&Ja.\.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\launch-EN7506e353034849faa4a18bc4c20e727c.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	145655
Entropy (8bit):	5.152273801869561
Encrypted:	false
SSDEEP:	3072:GuGxcHsup2LWDCYNMXCHwjUW+6r1GPG4xArt8SeyDmy:GPxtuiWDCYNWCHl6r1GPG4xy8SR
MD5:	2B805B5C38F6DE570AC8C1155D8BF2C3
SHA1:	2BB4C9B63CB17D7C912F6D00F8FE6D2D122F9465
SHA-256:	4C3D3C8A1143CFF82D98D4B3EC9D80FD4ABF23B0445F52EF1A85D975595C5769
SHA-512:	FCABFBF03DE35D78E1F2F8A11B6FAF468F9AF585AA05417B6BE49E16C5B83152BD1FF07F9105FB4C473AE5E9756FD01280AA44F31EB5D8E482FDA24C9A8DB8F0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/launch-EN7506e353034849faa4a18bc4c20e727c.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/launch-EN7506e353034849faa4a18bc4c20e727c.js`..window._satellite=window._satellite||{},window._satellite.container={buildInfo:{minified:!0,buildDate:"2021-01-12T23:39:06Z",environment:"production",turbineBuildDate:"2020-08-10T20:14:17Z",turbineVersion:"27.0.0"},dataElements:{"JSLL RedTiger":{defaultValue:"",modulePath:"core/src/lib/dataElements/customCode.js",settings:{source:function(){return 0<$("#primaryArea[data-m]").length&&awa.isInitialized}}},MSCC_Consent:{defaultValue:"",modulePath:"core/src/lib/dataElements/customCode.js",settings:{source:function(){return!("undefined"!=typeof window.mscc&&"function"==typeof window.mscc.hasConsent&&!window.mscc.hasConsent())}}},"Surface - All Pages":{defaultValue:"",modulePath:"core/src/lib/dataElements/customCode.js",settings:{source:function(){return!(!location.pathname.match(/\/..\-..\/surfaceV?/gi)||location.pathname.match(/\/..\-..\/surfaceV\/business\/?/gi))}}}},"Surface - EN-US

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\meBoot.min[1].js	
File Type:	ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	154427
Entropy (8bit):	5.55030568871564
Encrypted:	false
SSDEEP:	3072:9xTI1rl1dz269QXU9vfRYb6fGP9weLS1SP:3cVw6Kbx9FLS1SP
MD5:	C57C07C4674AE6F46031D21047D05989
SHA1:	A95BFD98F4698ED582A16395AC1FFD45961FD0E1
SHA-256:	DE6214A5477F1EE5BB72E015094923CAD51ED057A379BCEB817D82A9A1B0498D
SHA-512:	6ADBFB036C73F903DFA5F5C45B1B64B16E8791A57C23601A574B9CF804A452D03AFB446F8130A8F596382194FDFC1D752CA0821C35FE934BA1A31285F0865129
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://mem.gfx.ms/scripts/me/MeControl/10.20321.2/de-DE/meBoot.min.js
Preview:	MeControlDefine("meBoot",["exports","@mecontrol/web-inline"],function(t,A){"use strict";var s=function(){},i={},u=[],p=[];function w(t,e){var n,r,o,i,a=p;for(i=arguments.length;2<i--;)u.push(arguments[i]);for(e&&null!=e.children&&(u.length||u.push(e.children),delete e.children);u.length;)if((r=u.pop())&&void 0!==r.pop)for(i=r.length;i--;)u.push(r[i]);else"boolean"==typeof r&&(r=null),(o="function"!=typeof t)&&(null==r?r="":"number"==typeof r?r=String(r):"string"!=typeof r&&(o=!1)),o&&n?a[a.length-1]+=r:a===p?a=[r]:a.push(r),n=o;var c=new s;return c.nodeName=t,c.children=a,c.attributes=null==e?void 0:e,c.key=null==e?void 0:e.key,c}function T(t,e){for(var n in e)t[n]=e[n];return t}function d(t,e){t&&("function"==typeof t?t(e):t.current=e)}var e="function"==typeof Promise?Promise.resolve().then.bind(Promise.resolve()):setTimeout;var l=/acit|ex(?:s|g|n|p|$)|rph|ows|mnc|ntw|ine[ch]|zoo|^ord/i,n=[];function a(t){!t._dirty&&(t._dirty=!0)&&1==n.push(t)&&e(r)}function r(){for(var t;t=n.pop();)t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\meCore.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	102316
Entropy (8bit):	5.253265102841877
Encrypted:	false
SSDEEP:	3072:I7uoUCePnnlneqFpJrJjsV72lzTPH/cTOhGyEo7oYnOG:2WleMXLGyEo7oYnOG
MD5:	3363B2464B87874E9A00DC495CD48F4A
SHA1:	998C3406DDB1076E076E5D1D137B101DA6962222
SHA-256:	1CE215BA87D643ED5977E31E5AA1670952888504F2521A56668C7A0D9B15E8FB
SHA-512:	A9E19CFACE0E80FFF076C77763220038DE15F110D8F49662D1F13260FEE99A82055B2753540B1D6E121BD2D27A0CCD48EC598954BB3023CE04DF1644449EB8F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://mem.gfx.ms/scripts/me/MeControl/10.20321.2/de-DE/meCore.min.js
Preview:	MeControlDefine("meCore",["exports","@mecontrol/web-inline","@mecontrol/web-boot"],function(t,f,h){"use strict";var r=function(t,e){return(r=Object.setPrototypeOf||{__proto__:[]}instanceof Array&&function(t,e){t.__proto__=e}||function(t,e){for(var n in e)e.hasOwnProperty(n)&&(t[n]=e[n])})(t,e)};function e(t,e){function n(){this.constructor=t}r(t,e),t.prototype=null===e?Object.create(e):(n.prototype=e.prototype,new n)}var d=function(){return(d=Object.assign||function(t){for(var e,n=1,r=arguments.length;n<r;n++)for(var o in e=arguments[n])Object.prototype.hasOwnProperty.call(e,o)&&(t[o]=e[o]);return t}).apply(this,arguments)},s=function(){},i={},u=[],l=[];function v(t,e){var n,r,o,i,a=l;for(i=arguments.length;2<i--;)u.push(arguments[i]);for(e&&null!=e.children&&(u.length||u.push(e.children),delete e.children);u.length;)if((r=u.pop())&&void 0!==r.pop)for(i=r.length;i--;)u.push(r[i]);else"boolean"==typeof r&&(r=null),(o="function"!=typeof t)&&(null==r?r="":"number"==typeof r?r=String(r):"s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\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):	41280
Entropy (8bit):	5.4414493584466115
Encrypted:	false
SSDEEP:	384:887XrUJds35bd8cA8tF87XrUJds35bd8cA8t287XrUJds35bd8cA8tY87XrUJdsV:dw25ruw25rVw25r7w25rz
MD5:	175817CA50618A049ED4DB9CB6AADAED
SHA1:	F5685E27351D73A138A7EBD96C1890C45548C0DA
SHA-256:	EBD33FA81F4BFBE3D16166346E94D4CFFBBBEB6BBBCFFA0E4C80390DDA6B8D14
SHA-512:	7200A2E82FCDFE0464D98DB2BF5E937E4ADE37A3E5261F408B70D35B3FAD74B8F7F852035E9728E62A1C7A10285D15E6BBD9080D317BC2C4DEEEBD0CCE6DBA72
Malicious:	false
Reputation:	low
Preview:	Copyright (C) Microsoft Corporation. All rights reserved. --><!DOCTYPE html> ServerInfo: BY1PPF5DD46BCCD 2021.01.08.00.05.12 Live1 Unknown LocVer:0 --> PreprocessInfo: 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://login.live.com/pp1600/"/><noscript><meta http-equiv="Refresh" content="0; URL=https://login.live.com/jsDisabled.srf?mkt=EN-US&lc=1033&uaid=42242b5300c74e9e388bb2dac07a2251"/>Microsoft account requires JavaScript to sign in. This web browser either does not support JavaScript, or scripts are being blocked. To find out whether your browser supports JavaScript, or to allow scripts, see the browser's online help.</noscript><title>Windows Live ID</title><meta name="robots" content="none" /><meta name="PageID" con

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\microsoft-logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\microsoft-logo[1].png	
File Type:	PNG image data, 226 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	3331
Entropy (8bit):	7.927896166439245
Encrypted:	false
SSDEEP:	96:zHjOKn3csE3x5liVsCo4GcPIZpV6x5cge8oo9:zDOK3zE3x5TCwcP4LQNeq
MD5:	EF884BDEDEF280DF97A4C5604058D8DB
SHA1:	6F04244B51AD2409659E267D308B97E09CE9062B
SHA-256:	825DE044D5AC6442A094FF95099F9F67E9249A8110A2FBD57128285776632ADB
SHA-512:	A083381C53070B65B3B8A7A7293D5D2674D2F6EC69C0E19748823D3FDD6F527E8D3D31D311CCEF8E26FC531770F101CDAF95F23ECC990DB405B5EF48B0C91B2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cmrinsure-my.sharepoint.com/_layouts/15/images/microsoft-logo.png
Preview:	.PNG.....IHDR.....0.....sRGB.....IDATx..=w....G.z..L.4fN.k\dS..._`.....r...~.F..e._.RZ.0.K.\..CB...1.{qq/..^|.G..o.....?....Or.....y~....]..V.a.mM...M.\k*H..@B`s.$"n ...)!.@"b#4. !.9...7.u...hD ....T.....:EJ.4"..X.....<\|.pgkk+....>~.....pju1i"b.J.&!.!...=T....k..D7.....O.<.?}...../..(.`0..!.C..'.?..e..~.....l6...._.x1rmR...$|E...l.WKDH...f..... ...Y.0R... .>...{...-..o.....,...E../....._....eM.Q....@Q...w sp5.9..l.W)...Pq... .]..B..).../M.G.g....].V...5$<.....Eb.9.....>LYAk.Z.k..b..]N%>}4a....4!S...t..d..<.8AH+.../r...._...!qt.:q..fR.:.. KW..._...T...5..>.0!.hq.rbND\...XR.,2.uX..Q.b...wQ.....g..X...F...~.....ikZE...UA....V.l!..]..Mm..R.....~k.VC.n..V.*B#W...\..yI.3.....2.....6c....2J....,g..5O1.s.4V2.....f..K..Obf\....;.w ...\|.F>F>6_z..P.dU<.wVV.....?.q.?&.....O.>....l.S.upp....59.C_.....fJ.M.={v,.....]Y_....n.?UF....v<.$..AD...p.....:$r =p...C.k.3....n.v..~.TGd!...l.W...s..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\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):	5.292241195528751
Encrypted:	false
SSDEEP:	1536:BHmIR3dEJ9Zm4nzKF5ZHgKh1LGYhz3jEj9TNfHx7EmI9o/c+7YupJypWqxWCtj6Q:BlR3diLU4Y0c+7YupJypNtWfY
MD5:	B5BDF065A890544C4B0E032FFBFAC269
SHA1:	A699C2088A15DBDB0B558E0D297D9D80317822C5
SHA-256:	2E55681BB82CABFADF28F18EA0B39F3F911FC828DE313E6604B44149E8FAF200
SHA-512:	90E14695F03180EE0BDE737FA659B92A7BAC26003574EB79169A96EA23B9C0D8D79C997EAD4CDE85C894805246AD98C431804BBBBCB0B6076E0086C43EA6EA36
Malicious:	false
Reputation:	low
Preview:	.....<!DOCTYPE html>..<html lang="en-us" dir="ltr">..<head data-info="{"v":"1.0.7662.39393","a":"e2777f5d-af7a-4270-a950-f57d3708a15e","cn":"OneDeployContainer","az":"{did:92e7dc58ca2143cfb2c818b047cc5cd1, rid: OneDeployContainer, sn: marketingsites-prod-odnortheurope, dt: 2018-05-03T20:14:23.4188992Z, bt: 2020-12-24T05:53:06.0000000Z}","ddpi":"1","dpio":"","dpi":"1","dg":"uplevel.web.pc.ie","th":"default","m":"en-us","l":"en-us","mu":"en-us","rp":"/en-us/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\user\AppData\Local\Microsoft\Windows\INetCache\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):	298040
Entropy (8bit):	5.170582206405612
Encrypted:	false
SSDEEP:	3072:09GZg9tIQHj9b1skD1nPwwwW9/xNS/xg4DJ3P26:09GrW9/DCW9Yhu6
MD5:	9CA3E3920A1FB6F3A5D3FA1F40DA56F0
SHA1:	F4AC5E5BA4422919F4CC9A8499D672754F840CE4
SHA-256:	A5E5538AB72F6C15A94665A0828BECCE000BD96113DD7CBF877FB169CCE809AA
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:	/*! 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.options.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=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?l.className.baseVal=t:l.className=t)}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\mwf-main.umd.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\mwf-main.umd.min[1].js	
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	361058
Entropy (8bit):	5.174653163091536
Encrypted:	false
SSDEEP:	3072:X660y74FC9UP93rLgW99dQwWFroVSz88/CiDlmKsUCFpuOxRxAc:X660y6C9m78W9n1WF8Mf/qUcRz
MD5:	A8FB1CBEEC229F17B436F41A022B08F4
SHA1:	D1BF3D470586F0485D7366FE718BEF5C6D5EA797
SHA-256:	D944ECBDA705212F75DFA94D7F0ED5E54F117079CFBBE266572F55175C5253EC
SHA-512:	C4BE75C897996EEFD72EEB46326912322347FA526BE102DC3CCBD50BFECD2389B9DC2F3DF8648EED40C19AA1E2ED871B90B4224DC25CF0C4A595F60E72578/58
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://mwf-service.akamaized.net/mwf/js/bundle/1.57.8/mwf-main.umd.min.js
Preview:	/*! modernizr 3.3.1 (Custom Build) | MIT *. * https://modernizr.com/download/?-eventlistener-picture-printshiv-setclasses !*/.!function(n,t){function h(n,t){return typeof n===t}function c(){var u,n,f,e,o,c,t;for(var l in r)if(r.hasOwnProperty(l)){if(u=[],n=r[l],n.name&&(u.push(n.name.toLowerCase()),n.options&&n.options.aliases&&n.options.aliases.length))for(f=0;f<n.options.aliases.length;f++)u.push(n.options.aliases[f].toLowerCase());for(e=h(n.fn,"function")?n.fn():n.fn,o=0;o<u.length;o++)c=u[o],t=c.split(".."),1===t.length?i[t[0]]=e:(!i[t[0]]||i[t[0]]instanceof Boolean||i[t[0]]=new Boolean(i[t[0]])),i[t[0]][t[1]]=e),s.push((e?"":"no-")+t.join("-"))}function l(n){var t=u.className,r=i._config.classPrefix||"",e;(f&&(t=t.baseVal),i._config.enableJSClass)&&(e=new RegExp("(^|\\s)"+r+"no-js(\\s|$)"),t=t.replace(e,"$1"+r+"js$2"));i._config.enableClasses&&(t+=" "+r+n.join(" "+r),f?u.className.baseVal=t:u.className=t)}var s=[],r=[],o={_version:"3.3.1",_config:{classPrefix:"",enableClasses:!0,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\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/ltcpKR3+MMrOfF:MSVI/BvVclQPH
MD5:	0757357BA2567A518EAF8EB0723677E1
SHA1:	CC3EB31A04544F1A7257A0810FA09576E56035CB
SHA-256:	ED8A2123175AE5DBEC6A22DA8B479DACDA8F255FC21274A40ABFA7E7B6EB5676
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:	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__)./***

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\mwfmdl2-v3.54[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26288, version 0.0
Category:	downloaded
Size (bytes):	26288
Entropy (8bit):	7.984195877171481
Encrypted:	false
SSDEEP:	768:56JqQaQphRbTHiKNF5z/02h5KpJW3pPOA8Y9g/:gdTTH5XKpJWdH1W/
MD5:	D0263DC03BE4C393A90BDA733C57D6DB
SHA1:	8A032B6DEAB53A33234C735133B48518F8643B92
SHA-256:	22B4DF5C33045B645CAFA45B04685F4752E471A2E933BFF5BF14324D87DEEE12
SHA-512:	9511BEF269AE0797ADDF4CD6F2FEC4AD0C4A4E06B3E5BF6138C7678A203022AC4818C7D446D154594504C947DA3061030E82472D2708149C0709B1A070FDD0E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/mwf/_h/v3.54/mwf.app/fonts/mwfmdl2-v3.54.woff
Preview:	wOFF.....f.....D.....OS/2...X...H...`JM.FVDMX.....^.qcmap.....*.9cvt ...4... ...*....fpgm...T.....Y...gasp...D.....glyf...P..U5.....head..]....2...6..Chhea..]....$$...hmtx..]....ye'loca..^.....Gmaxp..`.... ... ./..name..`....8....]..Rpost..f..... .Q.wprep..f$.....x...x.c`.Pf.....:....Q.B3_dHc..`e.bdb... .`@..`...../9.\|...V...)00...-.Wx...S....._..m.m.m.m;e..y.~.....<p..a.0t.&...a.pa.0B.1..F...Q.ha.0F.3....q.xa.0A.0L.&...I.da.0E.2L....i.ta.0C.1..f...Y.la.0G.3.....y.\|a..@X0,.....E.ba.DX2,....e.ra..BX1..V...U.ja..FX3.....u.za..A.0\|.6...M.fa.E.2\|....m.va..C.1..v...].na..G.3.....}.~a.p@80.....C.a..pD82.....c.q..pB81..N...S.i..pF83.....s.y..pA.0\.....K.e..pE.2\....k.u..pC.1..n...[.m..pG.3.....{.}...@x0<.....G.c...Dx2<....g.s...Bx1..^...W.k...Fx3.....w.{...A.0\|.>...O.g...E.2\|....o.w...C.1..~...._.o..08.....?..0$.....x...mL.U.....9.x.`[...&BF@X...V.h.Z..h.....`n....[..U

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\newsletter-icon[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\newsletter-icon[1].svg	
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1093
Entropy (8bit):	5.378834656577112
Encrypted:	false
SSDEEP:	24:2dpLATLf3vlbWwmhoAJnTIRL0pdxiWnE0oEzoEroEnn2:chAvf3vlbWwmh5Jy0MWLn3q
MD5:	DA6E674C3855E4C32F43543D0490E2D0
SHA1:	6F6F49CE32BDBA927A4646D19E74BC06BDBEE0A2
SHA-256:	0FE1530B059249BBAED30CA5594D77F442BF7072E4AA39404F921EB281B2926B
SHA-512:	66FFCEA829A8B3738A049E482D9835FB4A92D15B877C48EF5E7C83FE17C278D38301D1272AB3F332FB651E3FD8DCFE9474B329522CB17CD90C0E5CC6AF923F2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/newsletter-icon.svg?version=26094b8a-2cfc-fa19-5dfa-4a6913af6eb5
Preview:	<?xml version="1.0" encoding="utf-8"?>. Generator: Adobe Illustrator 20.1.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->.<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px".. viewBox="0 0 92 92" style="enable-background:new 0 0 92 92;" xml:space="preserve">.<style type="text/css">...st0{fill:#505050;}.</style>.<g>..<path class="st0" d="M78.2,27.2V16.4H3v48.7c0,5.8,4.7,10.5,10.5,10.5h64.8c5.9,0,10.8-4.8,10.8-10.8V27.2H78.2z M83.6,64.8...c0,3-2.4,5.4-5.4,5.4H13.5c-2.8,0-5.1-2.3-5.1-5.1V21.8h64.5v8.1v2.7v29.6c0,1.5,1.2,2.7,2.7,2.7c1.5,0,2.7-1.2,2.7-2.7V32.6h5.4...L83.6,64.8L83.6,64.8z"/>..<g>...<rect x="13.8" y="27.2" class="st0" width="53.8" height="5.4"/>..</g>..<g>...<rect x="46" y="59.4" class="st0" width="21.5" height="5.4" />..</g>..<g>...<rect x="46" y="48.7" class="st0" width="21.5" height="5.4"/>..</g>..<g>...<rect x="46" y="37.9" class="st0" width="21.5" height="5.4"/>..</g>..<g>...<path class=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\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:Udf0F+MOu2UOqD3426TKgR2Yyk9696TkMYqdfskeEkeGk/ksuF9qaSm9qags:Ud8FYqTj36TKgR2Yyk9696TkMYO0keEW
MD5:	A570448F8E33150F5737B9A57B6D889A
SHA1:	860949A95B7598B394AA255FE06F530C3DA24E4E
SHA-256:	0BD288D5397A69EAD391875B422BF2CBDCC4F795D64AA2F780AFF45768D78248
SHA-512:	217F971A8012DE8FE170B4A20821A52FA198447FA582B82CF221F4D73E902C7E3AA1022CB0B209B6679C2EAE0F10469A149F510A6C2132C987F46214B1E2BBBC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://statics-marketingsites-wcus-ms-com.akamaized.net/statics/override.css?c=7
Preview:	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, SegoeUI,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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\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):	75048
Entropy (8bit):	5.208191089349092
Encrypted:	false
SSDEEP:	768:vYtBTN6uayKTFKSsKQgGsckLkEuFEoW1G9ottlliGicPRuDdueyaaFpdaHqGQKeJ:vYtn6HyrsmjNJ
MD5:	67F7DB063DB58778065F6BDCB48FD328
SHA1:	7A1836804AED81509D2E47E27EE64E25C9386BC5
SHA-256:	7113888F41B75E72918A5073C227A7049A2B76DA626B74C4D9762DC4A9A3CB52
SHA-512:	0E2D30951A353BCE5A4909346B8536779B0D4C1C71F06CBAC14FA34911E51CA5EE9C16709E8201DB8563730C8B90709A64BA87116B76271560B823A3737E3101
Malicious:	false
Reputation:	low
Preview:	.<!DOCTYPE html ><html xmlns:mscom="http://schemas.microsoft.com/CMSvNext" xmlns:md="http://schemas.microsoft.com/mscom-data" lang="en-us" xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta charset="utf-8" /><meta name="viewport" content="width=device-width, initial-scale=1.0" /><link rel="shortcut icon" href="//www.microsoft.com/favicon.ico?v2" /><script type="text/javascript" src="https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js">.. // Third party scripts and code linked to or referenced from this website are licensed to you by the parties that own such code, not by Microsoft. See ASP.NET Ajax CDN Terms of Use - http://www.asp.net/ajaxlibrary/CDN.ashx... </script><script type="text/javascript" language="javascript">/*<![CDATA[*/if($(document).bind("mobileinit",function(){$.mobile.autoInitializePage=!1}),navigator.userAgent.match(/IEMobile\/10\.0/)){var msViewportStyle=document.createElement("style");msViewpor

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\privacy[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):	51578
Entropy (8bit):	5.103165227041674
Encrypted:	false
SSDEEP:	768:UMZxy8WiAEZAEGhAZgmu5RPP5m5SuUgRfnJYN9IYyEnc0BE:ZTypnhIgmu5RYBHE+
MD5:	04E64F110B3EA8F013A6746075A194DB
SHA1:	F04685516041DB32757E3A5CC3A9190E44277CD1
SHA-256:	9146DD7257209EC6185205E52DA0AB4B98267F670AD75A08F83FF61279B704A6
SHA-512:	FF3F7424BCE3133DCD8EC5D83DCAA1AA35B0F9566F1A7052172CBF58F4166756009F7D4C4C462825A99309E5FE16E8F4897F3DA28538EFC2B9504277A2EB927
Malicious:	false
Reputation:	low
Preview:	..<!DOCTYPE html>..<html dir="ltr" lang="en-US" data-role-name="MeePortal" class="ltr SignedOut-privacyPage signedout js">..<head>.. <title>Microsoft account | Microsoft Account Privacy Settings</title>.... <meta http-equiv="X-UA-Compatible" content="IE=edge">.. <meta charset="utf-8" />.. <meta name="viewport" content="width=device-width, initial-scale=1.0" />.. <meta name="format-detection" content="telephone=no" />.. <meta name="description" content="Microsoft allows you to control your account your way with customizable privacy settings. Manage your Xbox, Windows, and other privacy settings on this page." />.. <meta name="pageid" content="SignedOut-privacyPage" />.. <meta name="Keywords" content="microsoft privacy, microsoft privacy settings, microsoft account privacy" />.. <meta name="robots" content="index, follow" />.. <meta name="og:site_name" content="Microsoft" />.. <meta name="og:type" content="website" />.. <met

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\signedout-oneui[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	4550
Entropy (8bit):	5.0524612791133245
Encrypted:	false
SSDEEP:	96:uNo8sEjppapAekH5LVMGalJavLuqIhJqHw3+wr7ksB+:uNoxoXapAnD9cHA+87hB+
MD5:	F0F10ACB5C773537A505153575D787F7
SHA1:	4B50C47AB36A9E3665F3B8ED0BE1CEA299660520
SHA-256:	B526A7C4C93C6F021FE504526F64A908CAF9CC4A24507D1BC68DD439DDFF8130
SHA-512:	F447DFEDBA66564271330619851F1109F569660DD944B9DAEC24B0B561F2CA7B608463C10A1511CF9E140073EE5EBC4DA420B6557F3AC279C551A3F718F19E40
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://account.microsoft.com/bundles/styles/signedout-oneui?v=89Yl1rC3PCtb9BEGzRj1ZxU7qt1MVdvgIpMjJPR4snM1
Preview:	.mee-icon{color:#000}.mee-icon.mee-icon-WindowsLogo{color:#0067b8}.mee-icon.mee-icon-SkypeLogo{color:#1ab2e7}.mee-icon.mee-icon-XboxLogo{color:#197d3e}.mee-icon.mee-icon-OfficeLogo{color:#d84126}.mee-icon.mee-icon-BingLogo{color:#0c8484}.mee-icon.mee-icon-TeamsLogo{color:#4b53bc}.mee-icon.mee-icon-NewsLogo{color:#f03442}.rich-para span.mee-icon{color:inherit}[class^="m-"]+.m-hero-item{margin-top:0;float:none}[class^="m-"]+.m-feature{padding-top:0;margin-top:0}.c-link-navigation img{width:60px;height:60px}.m-banner h2{padding-top:0}.m-banner{background:#0067b8;color:#fff;padding-bottom:48px;max-width:none}#signinfooter{color:#fff;padding-left:24px;white-space:normal}@media screen and (-ms-high-contrast:black-on-white){#signinfooter{color:#00009f}}[data-icon]:before{content:attr(data-icon);font-family:'Membership Icons'}div[data-grid~="container"]+div[data-grid~="container"]:nth-of-type(2n){background-color:#e3e3e3}div[data-grid~="container"]{padding:38px 5%}.privacy-other .item{display:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\site[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	131306
Entropy (8bit):	5.31725447413608
Encrypted:	false
SSDEEP:	1536:jloFM2JfgcRF9h0KpR3E78Jm8Ld8g3SgWHFBF1x79xpkk//W3197t0EDKQqdF+2s:KD2DBF1r/W3197t0EDkdF+Tq8
MD5:	CAC8CF07AE4CC2E03C3057C040DBA5C4
SHA1:	1CD7F6F04F82CF4A54204D77444876200AF4B9DC
SHA-256:	46287E3C8FC4FE616BEE38AC9B25FCF1B5361119758C848D1DC67C8D69F105FB
SHA-512:	1397EF4F12687414060EA66F8C40A707108980070FDE9A83C91970B126B9970EA90F5CEA12C6FC2ACFA81976B40C542CBF646CED71350ADC5B316D1CCCD5A5F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://account.microsoft.com/bundles/scripts/site?v=1pBuGSHwiVz6rvFZTA9oWFVo2_SjkX_9CmwoXWhQZe01
Preview:	function bingMapLoaded(){MeePortal.BingMapWaiter.mapsLoaded()}var Helpers,inputWidth,mq,WebHip,MeePortal;(function(n,t){typeof exports=="object"&&typeof module!="undefined"?t(exports):typeof define=="function"&&define.amd?define(["exports"],t):t(n.cookieManager=n.cookieManager||{})})(this,function(n){"use strict";function o(n){return n.replace(e,"")}var u=63072e6,t=window,i=window,r=function(){function n(n){var u=this,t,i,r;this.localDocument=n;this.nonEssentialCookies=[];this.previouslyConsentedCookies=[];this.isMsccCallbackRegistered=!1;this.isWCPCallbackRegistered=!1;this.isInFlightGCookieBanner=!1;r=(i=(t=window.MeePortal)===null||t===void 0?void 0:t.g_userFlights)!==null&&i!==void 0?i:[];r.forEach(function(n){n.toLowerCase()==="gcookiebanner"&&(u.isInFlightGCookieBanner=!0)})}return n.prototype.getCookie=function(n,t,i){var e,r,u;if(!n)throw new Error("CookieManager.getCookie - name argument should not be false-y");if(this.isInFlightGCookieBanner&&this.registerWCPCallback(),t&&!th

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\slider[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):	177086
Entropy (8bit):	5.096036264597187
Encrypted:	false
SSDEEP:	3072:GAwmeEZACGNeDN4o9WwqTatIjxrfdx811vWSltmZKVCgGHLR/3xnxHBzyP5kTP3B:CEZACA
MD5:	98CF407E0A5356981310CDD901567104
SHA1:	003999320D4CD3D39CC71F658CB722A3327A67C4
SHA-256:	BC3E59B72A6D0431BF9D1920F5CEF2A52F08A89EF6AB88B53CFFFAE093A92EF8
SHA-512:	C3C2DE3B53C90A738ADE3FA044018726F6323A424A150DDCA471A0A8F6C70151C53697E694DA1053BCA64CCEB4130D957CFE568957C6F6CAA25E596EFDE6EF ED
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/mwf/css/MWF_20201028_28422223/west-european/default/button/glyph/heading/image/list/pagebehaviors/selectmenu/slider?apiVersion=1.0&include_base=true
Preview:	@charset "UTF-8";./*! 1.57.0 | Copyright 2017 Microsoft Corporation | This software is based on or incorporates material from the files listed below (collectively, "Third Party Code"). Microsoft is not the original author of the Third Party Code. The original copyright notice and the license under which Microsoft received Third Party Code are set forth below together with the full text of such license. Such notices and license are provided solely for your information. Microsoft, not the third party, licenses this Third Party Code to you under the terms in which you received the Microsoft software or the services, unless Microsoft clearly states that such Microsoft terms do NOT apply for a particular Third Party Code. Unless applicable law gives you more rights, Microsoft reserves all other rights not expressly granted under such agreement(s), whether by implication, estoppel or otherwise.*/./*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */.html{font-family:sa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\social[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	465373
Entropy (8bit):	5.015480107121932
Encrypted:	false
SSDEEP:	3072:GAwmeEZACGszyP5kTP3bI0tfYqQ0xtLfj4ZDa813giY8R1j35Ap7zzN1n1JKfNkL:CEZACVw+fj
MD5:	3E80908AE0C097357DE76F75F751B9AC
SHA1:	AE67BAAD03731D13A353E4D1DC8AE25B255C95F4
SHA-256:	9EF31CF05A72EFCE450893B2D2B368B9E5C6910FAEF0CA81ABC3FCB7EFC395F5
SHA-512:	B072ACEAF58F7884057FE17909EE945F5F8F74B12C3748474FD5888D504DA70FF37FA2C1CFEFFBE8CFB4111233768B25BC4D29303C94CF0C6A9C6D609FA377C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/mwf/css/MWF_20201028_28422223/west-european/default/actiontoggle/alert/ambientvideo/areaheading/autosuggest/button/contentplacement/contentplacementitem/dialog/divider/drawer/glyph/heading/hero/heroitem/hyperlinkgroup/image/imageintro/list/mosaicplacement/multislidecarousel/pagebehaviors/productplacement/rating/skiptomain/social?apiVersion=1.0&include_base=true
Preview:	@charset "UTF-8";./*! 1.57.0 | Copyright 2017 Microsoft Corporation | This software is based on or incorporates material from the files listed below (collectively, "Third Party Code"). Microsoft is not the original author of the Third Party Code. The original copyright notice and the license under which Microsoft received Third Party Code are set forth below together with the full text of such license. Such notices and license are provided solely for your information. Microsoft, not the third party, licenses this Third Party Code to you under the terms in which you received the Microsoft software or the services, unless Microsoft clearly states that such Microsoft terms do NOT apply for a particular Third Party Code. Unless applicable law gives you more rights, Microsoft reserves all other rights not expressly granted under such agreement(s), whether by implication, estoppel or otherwise.*/./*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */.html{font-family:sa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\spoguestaccess-a0017cc2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	161989
Entropy (8bit):	5.339918222131445
Encrypted:	false
SSDEEP:	1536:Ieh9W6NxmcW/kCClKOY/Vu3PUEz45lLi6dhqumpWxaDaNrI9itUR3D7kLDbM:RWexEPqzELi0udRhD7B
MD5:	A0017CC26C936403E7606856755692A7
SHA1:	A87C65638A0FEBAA076F5316033BA08CDE5ED843
SHA-256:	08BD9EDCC17CC0B47080B229C0A88A4347000B2904A7F5DFFD37C7DD07A99C22
SHA-512:	39F5660CD3B04B5897E26DF416BF25301AB68E8BE130E6C863507DACA6356E76CC1ED1F1DF28639D34B391FC029D35D5C12F8398618E4CA5EE0225D9B1A7291
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spoprod-a.akamaihd.net/files/odsp-next-prod-amd_2020-12-04-sts_20210112.001/spoguestaccess-a0017cc2.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\spoguestaccess-a0017cc2[1].js	
Preview:	define("@fluentui/dom-utilities",["./dom-utilities/lib/index"],function(e){return e});.define("@fluentui/dom-utilities/lib/elementContains",["require","exports","./getParent"],function(e,t,n){"use strict";Object.defineProperty(t,"__esModule",{value:!0});t.elementContains=function(e,t,r){void 0===r&&(r=!0);var i=!1;if(e&&t)if(r)if(e===t)i=!0;else{i=!1;for(;t;){var s=n.getParent(t);if(s===e){i=!0;break}t=s}}else e.contains&&(i=e.contains(t));return i}});.define("@fluentui/dom-utilities/lib/elementContainsAttribute",["require","exports","./findElementRecursive"],function(e,t,n){"use strict";Object.defineProperty(t,"__esModule",{value:!0});t.elementContainsAttribute=function(e,t){var r=n.findElementRecursive(e,function(e){return e.hasAttribute(t)});return r&&r.getAttribute(t)}});.define("@fluentui/dom-utilities/lib/findElementRecursive",["require","exports","./getParent"],function(e,t,n){"use strict";Object.defineProperty(t,"__esModule",{value:!0});t.findElementRecursive=function e(t,r){re

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	471892
Entropy (8bit):	5.033188189125514
Encrypted:	false
SSDEEP:	12288:z+GWNnmKLewbOKV8cS+efSwCek2sPX6CnhLW4NXqwjMpGer10OYYuSYam:JWNnmKLewbOKV8cS+efSwCek2sPX6Cnf
MD5:	4255827860615CFCE59A1F9E92D27861
SHA1:	3E692FEAC8970F4FEC25DAA72B3BC59E82B3D8C8
SHA-256:	7CA5B7E5E358C5773236C8F0CB10F0F9B598408E1360611F0113E7433C855D73
SHA-512:	8A9848C273EDF70BA1E95BAF003D5AFBD650A1B8B2C1A157CDE280B919A29F86D307BBD3342425DD6E0022DA25DCE90153D5BBBDBA1BC7296F8E3F43A169E8E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSStyles/style.csx?k=d0881903-2097-5726-d782-43edaef8fec5_18686a99-0102-6c3c-3395-05d092772ffa_d31d3dbe-606e-a4d9-2b07-bdd563d0a288_9ee552ff-a934-d812-67bd-321f24428afe_752893cc-c41e-13b9-cb80-f26db496637f_de27edd8-7afb-41eb-1b6d-0d087c90f98f_83398ac8-1b1e-304e-969d-f792c4ff56b8
Preview:	.theme-light a.c-hyperlink.normal:active,.theme-light a.c-hyperlink.normal:hover,.theme-light a.c-hyperlink.normal{font-weight:normal !important}.surface-margin-top-120px{margin-top:50px}.high-contrast-mode .surface-hero-pivot-multi-img :not(.f-disabled).c-pivot>ul>a.f-active:focus{background:transparent}.surface-margin-bottom-120px{margin-bottom:80px}.overflow-x-hidden{overflow-x:hidden}html[lang="ar-qa"]{direction:rtl}html[lang="ar-qa"] a.m-skip-to-main,a.m-skip-to-main:hover{left:0}.zh-cn .surface-j-panes [data-accprodbuyid=""].surface-bg-cta-blue{display:none}.INTL-bussiness-product-placement li{width:50% !important;float:none !important;margin:0 auto}.surface-margin-bottom-34px{margin-bottom:34px}.surface-margin-top-40px{margin-top:30px}.responsive-surface-margin-bottom-120px{margin-bottom:100px}.surface-margin-top-112px{margin-top:115px}.surface-margin-top-64px{margin-top:64px}.surface-margin-top-20px{margin-top:20px}.responsive-surface-margin-top-70px{margin-top:55px}.cos_surfac

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\surface[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	163593
Entropy (8bit):	5.346101323173848
Encrypted:	false
SSDEEP:	1536:uGtutKojRFLHToVWVMAY30txV8UMd/U0ql3Us4fuI:uQ8KojRFLHTprEdt9s4f7
MD5:	AE5A746176A5FDA8367C55D9E8CE9830
SHA1:	CFFF559DB5BF5D1D35ADF8EDC7B5F27C843382B7
SHA-256:	CDCBA8F97B256E5F82D4CB82C8193BDBE24211EF08F55343E8FB14F1B928642C
SHA-512:	E3B7C0032327760F81C53A0CAA3E0A364A6134AA75B9C08A361C302CD3E1239162D8E321DD5DC2C9DF09AD656B757959804F0F82D31B7AFA49295B31F563FCB
Malicious:	false
Reputation:	low
Preview:	.<!DOCTYPE html ><html xmlns:mscom="http://schemas.microsoft.com/CMSvNext" xmlns:md="http://schemas.microsoft.com/mscom-data" class="grunticon skrollr skrollr-desktop" lang="en-us" xmlns="http://www.w3.org/1999/xhtml"><head> <meta content="width=device-width, initial-scale=1.0" name="viewport" /--> <mscom:conditional propertyexists="true" instancename="isCookieConsentRequired" customexpression="True::False"--> <script type="text/javascript" src="//www.microsoft.com/library/svy/min/pre_broker.js" async="true"></script>...<script type="text/javascript" src="//www.microsoft.com/library/svy/min/broker.js" async="true"></script--></mscom:conditional--><meta charset="utf-8" /><meta content="IE=edge,chrome=1" http-equiv="X-UA-Compatible" /><meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=5.0" /><link rel="shortcut icon" href="//www.microsoft.com/favicon.ico?v2" /><link rel="canonical" href="https://www.microsoft.com/en-us/surface"></link><

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\t[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	3.16293190511019
Encrypted:	false
SSDEEP:	3:CUmExltxlHh/:Jb/
MD5:	FC94FB0C3ED8A8F909DBC7630A0987FF
SHA1:	56D45F8A17F5078A20AF9962C992CA4678450765
SHA-256:	2DFE28CBDB83F01C940DE6A88AB86200154FD772D568035AC568664E52068363
SHA-512:	C87BF81FD70CF6434CA3A6C05AD6E9BD3F1D96F77DDDAD8D45EE043B126B2CB07A5CF23B4137B9D8462CD8A9ADF2B463AB6DE2B38C93DB72D2D511CA60E3B57E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\t[1].gif	
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\wcp-consent[1].js	
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):	255440
Entropy (8bit):	6.051861579501256
Encrypted:	false
SSDEEP:	6144:PIgagvUI0iDsW9Whsredo7NjIZjIZP0aNWgF9Dyjzh:PIgaHI0iIUedo7NjIZjIZP0o74t
MD5:	38B769522DD0E4C2998C9034A54E174E
SHA1:	D95EF070878D50342B045DCF9ABD3FF4CCA0AAF3
SHA-256:	208EDBED32B2ADAC9446DF83CAA4A093A261492BA6B8B3BCFE6A75EFB8B70294
SHA-512:	F0A10A4C1CA4BAC8A2DBD41F80BBE1F83D767A4D289B149E1A7B6E7F4DBA41236C5FF244350B04E2EF485FDF6EB774B9565A858331389CA3CB474172465EB3E F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wcpstatic.microsoft.com/mscc/lib/v2/wcp-consent.js
Preview:	var WcpConsent=function(e){var a={};function i(n){if(a[n])return a[n].exports;var o=a[n]={i:n,l:!1,exports:{}};return e[n].call(o.exports,o,o.exports,i),o.l=!0,o.exports}return i.m=e,i.c=a,i.d=function(e,a,n){i.o(e,a)||Object.defineProperty(e,a,{enumerable:!0,get:n})},i.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},i.t=function(e,a){if(1&a&&(e=i(e)),8&a)return e;if(4&a&&"object"==typeof e&&e&&e.__esModule)return e;var n=Object.create(null);if(i.r(n),Object.defineProperty(n,"default",{enumerable:!0,value:e}),2&a&&"string"!=typeof e)for(var o in e)i.d(n,o,function(a){return e[a]}.bind(null,o));return n},i.n=function(e){var a=e&&e.__esModule?function(){return e.default}:function(){return e};return i.d(a,"a",a),a},i.o=function(e,a){return Object.prototype.hasOwnProperty.call(e,a)},i.p="",i(i.s=1)}([function(e,a,i){window,e.exports=function(e){var a={};function i(n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\wdg-global.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	5805
Entropy (8bit):	5.278923653755367
Encrypted:	false
SSDEEP:	96:UKbTXTwvME3A3UmUZZH//iuLXFgH5XsrhUfGtA4DtPigKUZwr9reeKMQTesOnOsA:5bTXTwYwHn6C1UfGtzB6gvPzil3
MD5:	EF4613E3C20BFE5E3F07B49BD0B66C1E
SHA1:	EDE2835F716750EDC0245E2AF061732427F5A8ED
SHA-256:	3DC7C03D651B5E29363C365C3B83B83A508865A194639070A20ABD863FBBC054
SHA-512:	D8D6F060B4FCB2C781C8574BE01368BB8F25C314098BEF844859452DF88B77C9E7D088F190F111135F44C80F82F47F9AF4822240FEDEDD4F040F991CAE20EDC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWfyex
Preview:	(function(n,t,i){"use strict";./*!. * Some of the plugins here are extracted from WET. Details below.. * Web Experience Toolkit (WET) / Bo.te . outils de l'exp.rience Web (BOEW). * wet-boew.github.io/wet-boew/License-en.html / wet-boew.github.io/wet-boew/Licence-fr.html. * v4.0.25-development - 2017-05-04 . */.var r=t.wdg||{};r.doc=n(i);r.win=n(t);r.html=n("html");r.siteMuseCtaSelector=".mscom-link.c-call-to-action";r.modules=r.modules||{};r.jqEscape=function(n){return n.replace(/([;&,\.\+*\~':"\!\^\/#$%@\[\]\(\)=>|])/g,"\\$1")};r.modules.refactorSitemuseCtas=function(){n(r.siteMuseCtaSelector).contents().wrap("")};r.modules.setPrefooterDrawerInMobile=function(){n("#prefooterDrawer").click(function(){var t=n("#prefooterNav");n(this).attr("aria-expanded",!t.is(":visible"));n("#prefooterNav").slideToggle()})};r.modules.noCookieYTVideosWithConsent=function(){t.mscc&&(mscc.hasConsent()||n('iframe[src*="youtube.com"], [data-source*="youtube.com"], [data-youtube*="youtube.com"]

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\1-WebBrowsing-01[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 370, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	31965
Entropy (8bit):	7.9519959589170695
Encrypted:	false
SSDEEP:	768:G2+elgXGKSKgipe/3Nj2X8f2BS+oiJRKFYcWA:G2+esGKQiOcX2aSWc
MD5:	255DD67FA877795019867502F4095E85
SHA1:	0B3E8F077AA858C6F3613D1607CDF7BA699E6FE5
SHA-256:	BB88C60C19E587AD0793648DE59E089D35F424ECF0BFF9FD28CF33D16ED1A767
SHA-512:	96F6569C42781418C23B59F7209CF095BA5D54C47572B33B0F04DEA94DA1CD6882A6AF94241B09164CF518D66CC1D7739C834801CD62EBB252E1310C7186C818
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/1-WebBrowsing-01.png?version=280edfb3-3250-3e5d-5f4f-35711788a8a7

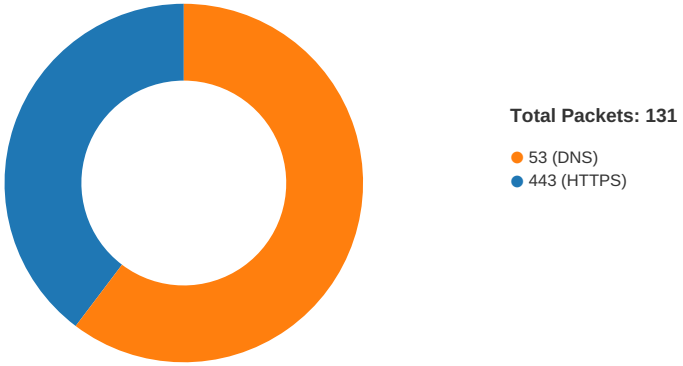
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\1-WebBrowsing-01[1].png	
Preview:	.PNG.....IHDR... ...r.....).....pHYs.....8".@...$zTXtCreator....sL.OJUpL+I-RpMKKM.)..Az..jz.... .IDATx...y.\.] .s.^U].U....e.%...o.....3d..0.....yC^`x.....d.$C..Y..qb..^c.I.-Kj. .}..k...3.\..j.^..R..~....{.....*..x.^..eg.....X...N..z...G..... .....0..X.....&.....d.`.....,.....A.....`2.....L..... .....0..X.....&.....d.`.....,.....A.....`2.....L..... .....0..X.....& ....p...x.g..cl..)...B...SJM9,...`#...za.%I.8.?3.c...I5.,UUu]7.,..... ...1.x<,...,..0..q...,B.z:....H .....|...<.1.q,.*...*L....p.(r.k...<o.IEQ.$.b/....2.`...X.Q..y<.|.....0EX....c#..,....'..BI... .....u.....a.I....,.c...p...J..0. p.W.q.b,... .....V.`YV....W.y^.4h.....J.f...<..zK8.Bo.+.{.....J.~.up..E"..eMo%.....,.c.F...+.Z...[..... .r=A.J{fp..e.....v..R.c.6.....6gk.K../.....c... ._....B..b[6.c4P._W..p..C.w"J...k..u...`.....u.....@..I...Y..n..<!DUUUU...|+.KF..Q.....l.....\.....(dA7.[!.)B.0R..g..]m.....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 19:10:58.288702965 CET	49722	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:58.288894892 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:58.434405088 CET	443	49722	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:58.434547901 CET	49722	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:58.434688091 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:58.434804916 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:58.441935062 CET	49722	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:58.443017006 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:58.588412046 CET	443	49722	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:58.588444948 CET	443	49722	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:58.588464022 CET	443	49722	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:58.588540077 CET	49722	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:58.588618040 CET	49722	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:58.589792967 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:58.589823008 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:58.589844942 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:58.589927912 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:58.590010881 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:58.634035110 CET	49722	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:58.634222031 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:58.641701937 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:58.780926943 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:58.781053066 CET	49723	443	192.168.2.3	52.104.14.25

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 19:10:58.782144070 CET	443	49722	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:58.782282114 CET	49722	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.133188963 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.322381973 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.413275957 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.413342953 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.413366079 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.413415909 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.413419008 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.413469076 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.413470030 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.413506985 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.413511992 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.413546085 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.413552999 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.413589001 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.413593054 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.413635015 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.413638115 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.413671970 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.413681984 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.413710117 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.413712025 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.413748980 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.413755894 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.413789988 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.413794041 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.413827896 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.413834095 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.413867950 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.413873911 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.413908958 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.413914919 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.413958073 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.413960934 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.414000034 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.559245110 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.559304953 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.559334993 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.559365034 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.559401989 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.559449911 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.559495926 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.559495926 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.559534073 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.559534073 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.559540033 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.559544086 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.559572935 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.559592009 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.559609890 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.559638023 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.559664011 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.569986105 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.577572107 CET	49722	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.590168953 CET	49725	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.590926886 CET	49726	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.591635942 CET	49727	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.720208883 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.720253944 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.720290899 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.720338106 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.720381021 CET	443	49723	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.720379114 CET	49723	443	192.168.2.3	52.104.14.25

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 19:10:59.720429897 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.720444918 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.720451117 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.720455885 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.724657059 CET	49723	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.728229046 CET	443	49722	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.728285074 CET	443	49722	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.728323936 CET	443	49722	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.728360891 CET	443	49722	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.728403091 CET	443	49722	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.728679895 CET	49722	443	192.168.2.3	52.104.14.25
Jan 13, 2021 19:10:59.737603903 CET	443	49727	52.104.14.25	192.168.2.3
Jan 13, 2021 19:10:59.737826109 CET	49727	443	192.168.2.3	52.104.14.25

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 19:10:52.737458944 CET	60100	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:10:52.788360119 CET	53	60100	8.8.8.8	192.168.2.3
Jan 13, 2021 19:10:53.898590088 CET	53195	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:10:53.946732044 CET	53	53195	8.8.8.8	192.168.2.3
Jan 13, 2021 19:10:55.163548946 CET	50141	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:10:55.214436054 CET	53	50141	8.8.8.8	192.168.2.3
Jan 13, 2021 19:10:56.632035017 CET	53023	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:10:56.680073023 CET	53	53023	8.8.8.8	192.168.2.3
Jan 13, 2021 19:10:57.025360107 CET	49563	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:10:57.082521915 CET	53	49563	8.8.8.8	192.168.2.3
Jan 13, 2021 19:10:58.177601099 CET	51352	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:10:58.253614902 CET	59349	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:10:58.273324966 CET	53	51352	8.8.8.8	192.168.2.3
Jan 13, 2021 19:10:58.301508904 CET	53	59349	8.8.8.8	192.168.2.3
Jan 13, 2021 19:10:59.581988096 CET	57084	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:10:59.640470982 CET	53	57084	8.8.8.8	192.168.2.3
Jan 13, 2021 19:10:59.796536922 CET	58823	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:10:59.854100943 CET	53	58823	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:01.063937902 CET	57568	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:01.120595932 CET	53	57568	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:06.945031881 CET	50540	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:06.995841980 CET	53	50540	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:08.092174053 CET	54366	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:08.140135050 CET	53	54366	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:09.243675947 CET	53034	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:09.302294016 CET	53	53034	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:11.463876963 CET	57762	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:11.511913061 CET	53	57762	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:13.683578968 CET	55435	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:13.731823921 CET	53	55435	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:14.422853947 CET	50713	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:14.562937021 CET	53	50713	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:21.196439981 CET	56132	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:21.247289896 CET	53	56132	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:24.276302099 CET	58987	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:24.342967033 CET	53	58987	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:27.016319990 CET	56579	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:27.064424992 CET	53	56579	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:27.635895967 CET	60633	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:27.683903933 CET	53	60633	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:28.024491072 CET	56579	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:28.086030006 CET	53	56579	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:28.454308033 CET	61292	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:28.521161079 CET	53	61292	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:28.633790016 CET	60633	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:28.692198038 CET	53	60633	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:28.907278061 CET	63619	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 19:11:28.964731932 CET	53	63619	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:29.042428017 CET	56579	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:29.090610981 CET	53	56579	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:29.652720928 CET	60633	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:29.700813055 CET	53	60633	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:30.081835985 CET	64938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:30.086674929 CET	61946	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:30.136312008 CET	64910	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:30.141608953 CET	53	64938	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:30.145612955 CET	53	61946	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:30.157114983 CET	52123	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:30.193844080 CET	56130	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:30.194650888 CET	53	64910	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:30.218173981 CET	53	52123	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:30.254304886 CET	53	56130	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:30.267798901 CET	56338	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:30.325131893 CET	53	56338	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:31.051403999 CET	56579	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:31.099522114 CET	53	56579	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:31.664813995 CET	60633	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:31.712631941 CET	53	60633	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:32.027055979 CET	59420	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:32.085040092 CET	53	59420	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:33.602303028 CET	58784	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:33.665471077 CET	53	58784	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:34.430309057 CET	63978	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:34.486866951 CET	53	63978	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:35.060692072 CET	56579	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:35.108592987 CET	53	56579	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:35.671770096 CET	60633	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:35.719516039 CET	53	60633	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:37.716809988 CET	62938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:37.780044079 CET	53	62938	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:38.286789894 CET	55708	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:38.334806919 CET	53	55708	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:39.849643946 CET	56803	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:39.865919113 CET	57145	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:39.866121054 CET	55359	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:39.881269932 CET	58306	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:39.909308910 CET	53	56803	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:39.925029039 CET	53	57145	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:39.931628942 CET	64124	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:39.931719065 CET	53	55359	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:39.937602043 CET	53	58306	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:39.989099026 CET	53	64124	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:41.118052006 CET	49361	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:41.165895939 CET	53	49361	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:41.944861889 CET	63150	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:42.017596006 CET	53	63150	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:42.285082102 CET	53279	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:42.359527111 CET	53	53279	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:42.733171940 CET	56881	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:42.804676056 CET	53	56881	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:43.757704020 CET	53642	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:43.805794001 CET	53	53642	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:51.413211107 CET	55667	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:51.473853111 CET	53	55667	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:55.805579901 CET	54833	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:55.865590096 CET	53	54833	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:56.119026899 CET	62476	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:56.177125931 CET	53	62476	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:58.287693024 CET	49705	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:58.335545063 CET	53	49705	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:59.299021006 CET	49705	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 19:11:59.346852064 CET	53	49705	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:59.624701023 CET	61477	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:59.687783957 CET	53	61477	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:59.725399971 CET	61633	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:59.734565973 CET	55949	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:11:59.784190893 CET	53	61633	8.8.8.8	192.168.2.3
Jan 13, 2021 19:11:59.795593977 CET	53	55949	8.8.8.8	192.168.2.3
Jan 13, 2021 19:12:00.315700054 CET	49705	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:12:00.363635063 CET	53	49705	8.8.8.8	192.168.2.3
Jan 13, 2021 19:12:00.696029902 CET	57601	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:12:00.780126095 CET	53	57601	8.8.8.8	192.168.2.3
Jan 13, 2021 19:12:02.318078995 CET	49705	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:12:02.367279053 CET	53	49705	8.8.8.8	192.168.2.3
Jan 13, 2021 19:12:06.326193094 CET	49705	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:12:06.374139071 CET	53	49705	8.8.8.8	192.168.2.3
Jan 13, 2021 19:12:09.729701996 CET	49342	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:12:09.870162010 CET	53	49342	8.8.8.8	192.168.2.3
Jan 13, 2021 19:12:10.751727104 CET	56253	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:12:10.761092901 CET	49667	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:12:10.765572071 CET	55439	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:12:10.768023014 CET	57069	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:12:10.770968914 CET	57659	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:12:10.817447901 CET	53	56253	8.8.8.8	192.168.2.3
Jan 13, 2021 19:12:10.825752974 CET	53	55439	8.8.8.8	192.168.2.3
Jan 13, 2021 19:12:10.825799942 CET	53	49667	8.8.8.8	192.168.2.3
Jan 13, 2021 19:12:10.828433037 CET	53	57659	8.8.8.8	192.168.2.3
Jan 13, 2021 19:12:10.840416908 CET	53	57069	8.8.8.8	192.168.2.3
Jan 13, 2021 19:12:12.717885017 CET	54717	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:12:12.788225889 CET	53	54717	8.8.8.8	192.168.2.3
Jan 13, 2021 19:12:17.540246964 CET	63975	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:12:17.557307005 CET	56639	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:12:17.559317112 CET	51856	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:12:17.560007095 CET	56546	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:12:17.561145067 CET	62152	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:12:17.561238050 CET	53470	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:12:17.561290026 CET	56446	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:12:17.578677893 CET	59631	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:12:17.599205017 CET	53	63975	8.8.8.8	192.168.2.3
Jan 13, 2021 19:12:17.616122007 CET	53	51856	8.8.8.8	192.168.2.3
Jan 13, 2021 19:12:17.619200945 CET	53	53470	8.8.8.8	192.168.2.3
Jan 13, 2021 19:12:17.619247913 CET	53	56446	8.8.8.8	192.168.2.3
Jan 13, 2021 19:12:17.619275093 CET	53	56546	8.8.8.8	192.168.2.3
Jan 13, 2021 19:12:17.622720957 CET	53	62152	8.8.8.8	192.168.2.3
Jan 13, 2021 19:12:17.636976957 CET	53	59631	8.8.8.8	192.168.2.3
Jan 13, 2021 19:12:17.638890982 CET	53	56639	8.8.8.8	192.168.2.3
Jan 13, 2021 19:12:45.012459040 CET	55515	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:12:45.060960054 CET	53	55515	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 19:10:58.177601099 CET	192.168.2.3	8.8.8.8	0x515b	Standard query (0)	cmrinsure-my.sharepoint.com	A (IP address)	IN (0x0001)
Jan 13, 2021 19:10:59.796536922 CET	192.168.2.3	8.8.8.8	0xd223	Standard query (0)	spoprod-a.akamaihd.net	A (IP address)	IN (0x0001)
Jan 13, 2021 19:11:14.422853947 CET	192.168.2.3	8.8.8.8	0x1243	Standard query (0)	cmrinsure-my.sharepoint.com	A (IP address)	IN (0x0001)
Jan 13, 2021 19:11:30.081835985 CET	192.168.2.3	8.8.8.8	0x8cbc	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Jan 13, 2021 19:11:30.193844080 CET	192.168.2.3	8.8.8.8	0x1d80	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)
Jan 13, 2021 19:11:39.931628942 CET	192.168.2.3	8.8.8.8	0xee6	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)
Jan 13, 2021 19:11:42.733171940 CET	192.168.2.3	8.8.8.8	0x5d90	Standard query (0)	logincdn.msauth.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 19:11:43.757704020 CET	192.168.2.3	8.8.8.8	0x8a82	Standard query (0)	aka.ms	A (IP address)	IN (0x0001)
Jan 13, 2021 19:11:56.119026899 CET	192.168.2.3	8.8.8.8	0xd58	Standard query (0)	amp.azure.net	A (IP address)	IN (0x0001)
Jan 13, 2021 19:11:59.725399971 CET	192.168.2.3	8.8.8.8	0x6d2d	Standard query (0)	assets.adobedtm.com	A (IP address)	IN (0x0001)
Jan 13, 2021 19:12:00.696029902 CET	192.168.2.3	8.8.8.8	0x682d	Standard query (0)	offertoolataprod.blob.core.windows.net	A (IP address)	IN (0x0001)
Jan 13, 2021 19:12:09.729701996 CET	192.168.2.3	8.8.8.8	0x578a	Standard query (0)	surfaceselfserviceoffertool.azurewebsites.net	A (IP address)	IN (0x0001)
Jan 13, 2021 19:12:10.751727104 CET	192.168.2.3	8.8.8.8	0x27cb	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)
Jan 13, 2021 19:12:10.765572071 CET	192.168.2.3	8.8.8.8	0x2807	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)
Jan 13, 2021 19:12:10.768023014 CET	192.168.2.3	8.8.8.8	0x9168	Standard query (0)	microsoftwindows.112.2o7.net	A (IP address)	IN (0x0001)
Jan 13, 2021 19:12:17.540246964 CET	192.168.2.3	8.8.8.8	0xf53	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)
Jan 13, 2021 19:12:17.557307005 CET	192.168.2.3	8.8.8.8	0x42a7	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)
Jan 13, 2021 19:12:17.561145067 CET	192.168.2.3	8.8.8.8	0x6671	Standard query (0)	statics-wcus.onestore.ms	A (IP address)	IN (0x0001)
Jan 13, 2021 19:12:17.561238050 CET	192.168.2.3	8.8.8.8	0x5ca9	Standard query (0)	statics-eus.onestore.ms	A (IP address)	IN (0x0001)
Jan 13, 2021 19:12:17.561290026 CET	192.168.2.3	8.8.8.8	0x91ec	Standard query (0)	statics-eas.onestore.ms	A (IP address)	IN (0x0001)
Jan 13, 2021 19:12:17.578677893 CET	192.168.2.3	8.8.8.8	0xc8fb	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 19:10:58.273324966 CET	8.8.8.8	192.168.2.3	0x515b	No error (0)	cmrinsure-my.sharepoint.com	cmrinsure.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:10:58.273324966 CET	8.8.8.8	192.168.2.3	0x515b	No error (0)	cmrinsure.sharepoint.com	698-ipv4e.clump.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:10:58.273324966 CET	8.8.8.8	192.168.2.3	0x515b	No error (0)	698-ipv4e.clump.prod.aa-rt.sharepoint.com	18980-ipv4e.farm.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:10:58.273324966 CET	8.8.8.8	192.168.2.3	0x515b	No error (0)	18980-ipv4e.farm.prod.aa-rt.sharepoint.com	18980-ipv4.farm.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:10:58.273324966 CET	8.8.8.8	192.168.2.3	0x515b	No error (0)	18980-ipv4.farm.prod.aa-rt.sharepoint.com		52.104.14.25	A (IP address)	IN (0x0001)
Jan 13, 2021 19:10:59.854100943 CET	8.8.8.8	192.168.2.3	0xd223	No error (0)	spoprod-a.akamaihd.net	spoprod-a.akamaihd.net.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:11:14.562937021 CET	8.8.8.8	192.168.2.3	0x1243	No error (0)	cmrinsure-my.sharepoint.com	cmrinsure.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:11:14.562937021 CET	8.8.8.8	192.168.2.3	0x1243	No error (0)	cmrinsure.sharepoint.com	698-ipv4e.clump.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:11:14.562937021 CET	8.8.8.8	192.168.2.3	0x1243	No error (0)	698-ipv4e.clump.prod.aa-rt.sharepoint.com	18980-ipv4e.farm.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:11:14.562937021 CET	8.8.8.8	192.168.2.3	0x1243	No error (0)	18980-ipv4e.farm.prod.aa-rt.sharepoint.com	18980-ipv4.farm.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:11:14.562937021 CET	8.8.8.8	192.168.2.3	0x1243	No error (0)	18980-ipv4.farm.prod.aa-rt.sharepoint.com		52.104.14.25	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 19:11:30.141608953 CET	8.8.8.8	192.168.2.3	0x8cbc	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:11:30.254304886 CET	8.8.8.8	192.168.2.3	0x1d80	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:11:38.334806919 CET	8.8.8.8	192.168.2.3	0x429a	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:11:39.937602043 CET	8.8.8.8	192.168.2.3	0xe86f	No error (0)	consentdeliveryfd.azurefd.net	star-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:11:39.989099026 CET	8.8.8.8	192.168.2.3	0xee6	No error (0)	mem.gfx.ms	cdn.account.microsoft.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:11:42.804676056 CET	8.8.8.8	192.168.2.3	0x5d90	No error (0)	logincdn.msauth.net	lgincdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:11:42.804676056 CET	8.8.8.8	192.168.2.3	0x5d90	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)
Jan 13, 2021 19:11:43.805794001 CET	8.8.8.8	192.168.2.3	0x8a82	No error (0)	aka.ms		23.211.149.25	A (IP address)	IN (0x0001)
Jan 13, 2021 19:11:56.177125931 CET	8.8.8.8	192.168.2.3	0xd58	No error (0)	amp.azure.net	160c1.wpc.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:11:59.784190893 CET	8.8.8.8	192.168.2.3	0x6d2d	No error (0)	assets.adobedtm.com	cn-assets.adobedtm.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:12:00.780126095 CET	8.8.8.8	192.168.2.3	0x682d	No error (0)	offertooldataprod.blob.core.windows.net	blob.bl6prdstr14a.store.core.windows.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:12:00.780126095 CET	8.8.8.8	192.168.2.3	0x682d	No error (0)	blob.bl6prdstr14a.store.core.windows.net		52.239.152.74	A (IP address)	IN (0x0001)
Jan 13, 2021 19:12:09.870162010 CET	8.8.8.8	192.168.2.3	0x578a	No error (0)	surfaceselfserviceofofertool.azurewebsites.net	waws-prod-mwh-031.sip.azurewebsites.windows.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:12:09.870162010 CET	8.8.8.8	192.168.2.3	0x578a	No error (0)	waws-prod-mwh-031.sip.azurewebsites.windows.net	waws-prod-mwh-031.cloudapp.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:12:10.817447901 CET	8.8.8.8	192.168.2.3	0x27cb	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:12:10.825752974 CET	8.8.8.8	192.168.2.3	0x2807	No error (0)	mem.gfx.ms	cdn.account.microsoft.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:12:10.840416908 CET	8.8.8.8	192.168.2.3	0x9168	No error (0)	microsoftwindows.112.2o7.net		15.237.76.117	A (IP address)	IN (0x0001)
Jan 13, 2021 19:12:10.840416908 CET	8.8.8.8	192.168.2.3	0x9168	No error (0)	microsoftwindows.112.2o7.net		15.237.136.106	A (IP address)	IN (0x0001)
Jan 13, 2021 19:12:10.840416908 CET	8.8.8.8	192.168.2.3	0x9168	No error (0)	microsoftwindows.112.2o7.net		35.181.18.61	A (IP address)	IN (0x0001)
Jan 13, 2021 19:12:17.599205017 CET	8.8.8.8	192.168.2.3	0xf53	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:12:17.619200945 CET	8.8.8.8	192.168.2.3	0x5ca9	No error (0)	statics-eus.onestore.ms	statics.onestore.ms.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:12:17.619247913 CET	8.8.8.8	192.168.2.3	0x91ec	No error (0)	statics-eas.onestore.ms	statics.onestore.ms.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:12:17.622720957 CET	8.8.8.8	192.168.2.3	0x6671	No error (0)	statics-wcus.onestore.ms	statics.onestore.ms.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:12:17.636976957 CET	8.8.8.8	192.168.2.3	0xc8fb	No error (0)	statics-neu.onestore.ms	statics.onestore.ms.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 19:12:17.638890982 CET	8.8.8.8	192.168.2.3	0x42a7	No error (0)	mem.gfx.ms	cdn.account.microsoft.com.akadns.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 19:11:42.900295973 CET	192.229.221.185	443	192.168.2.3	49789	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 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jan 13, 2021 19:11:42.900830984 CET	192.229.221.185	443	192.168.2.3	49790	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jul 20 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Tue Jul 20 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jan 13, 2021 19:11:43.895900965 CET	23.211.149.25	443	192.168.2.3	49795	CN=go.microsoft.com, OU=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft IT TLS CA 5, OU=Microsoft IT, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US	CN=Microsoft IT TLS CA 5, OU=Microsoft IT, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Sep 06 21:37:21 CEST 2019 Fri May 20 14:53:03 CEST 2016	Mon Sep 06 21:37:21 CEST 2021 Mon May 20 14:53:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Microsoft IT TLS CA 5, OU=Microsoft IT, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri May 20 14:53:03 CEST 2016	Mon May 20 14:53:03 CEST 2024		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 13, 2021 19:11:43.896029949 CET	23.211.149.25	443	192.168.2.3	49796	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

System Behavior

Analysis Process: iexplore.exe PID: 3352 Parent PID: 792

General

Start time:	19:10:55
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:	0x7ff7fe350000
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: 2436 Parent PID: 3352

General

Start time:	19:10:56
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:3352 CREDAT:17410 /prefetch:2
Imagebase:	0xbb0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: dllhost.exe PID: 2148 Parent PID: 792

General

Start time:	19:11:13
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: 2148

General

Start time:	19:11:14
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

File Activities

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 4316 Parent PID: 3352

General

Start time:	19:11:26
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:3352 CREDAT:17418 /prefetch:2
Imagebase:	0xbb0000
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

Disassembly

Code Analysis