ID: 382560
Sample Name: 0204.gif.dll
Cookbook: default.jbs
Time: 09:54:30
Date: 06/04/2021
Version: 31.0.0 Emerald

Table of Contents

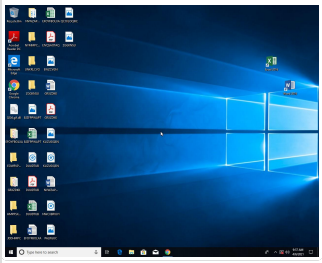
Analysis Report 0204.gif.dll

Overview

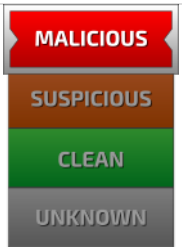
General Information

Sample Name:	0204.gif.dll
Analysis ID:	382560
MD5:	75c8d835dbb170..
SHA1:	12f7c7f15b85ef3…
SHA256:	8b130f9fbdcfc64…
Tags:	dll GG Gozi ISFB Ursnif
Infos:	

Most interesting Screenshot:



Detection



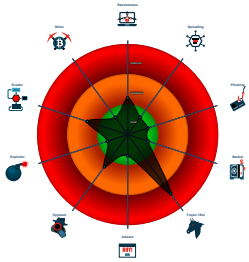
Ursnif

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Yara detected Ursnif
- Machine Learning detection for samp…
- Writes or reads registry keys via WMI
- Writes registry values via WMI
- Antivirus or Machine Learning detec…
- Contains functionality to call native f…
- Contains functionality to dynamically…
- Contains functionality to query CPU …
- Contains functionality to read the PEB
- Creates a DirectInput object (often fo…
- Creates a process in suspended mo…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6356 cmdline: loaddll32.exe 'C:\Users\user\Desktop\0204.gif.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6364 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\0204.gif.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6388 cmdline: rundll32.exe 'C:\Users\user\Desktop\0204.gif.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6376 cmdline: rundll32.exe C:\Users\user\Desktop\0204.gif.dll,StartService MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 5920 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6660 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5920 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 3440 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5920 CREDAT:17414 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 5184 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5216 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5184 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 3440 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5184 CREDAT:82948 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 5340 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 3228 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5340 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 3708 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5340 CREDAT:17414 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
[
  {
    "RSA Public Key":
"Om1HeBhXBR6NHvmWFG5B2kyl5mdcRMsb8ux2uo9VgGW0O2LzHZKk3w9bxw9stgphU0ayytcOYkK6GCNJlKSeMTZJ5WPgZiX+MaXiUccStEUTXkW1ubp0gdr16sb5U4M+rzWWPvc3s7bj9o1yqSJtP7PmMVp7E+3llLULQ9/DZbAD7SXa
ft6wcY8wFjSkI+8D"
  },
  {
    "c2_domain": [
      "bing.com",
      "update4.microsoft.com",
      "under17.com",
      "urs-world.com"
    ],
    "botnet": "5566",
    "server": "12",
    "serpent_key": "10301029JSJUYDWG",
    "sleep_time": "10",
    "SetWaitableTimer_value": "0",
    "DGA_count": "10"
  }
]
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.500504435.000000000562F000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.363000651.000000000582B000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.442401635.0000000003B4D000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.362707401.0000000003C4B000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000002.499116859.0000000003490000.00000004.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 16 entries				

Unpacked PEs

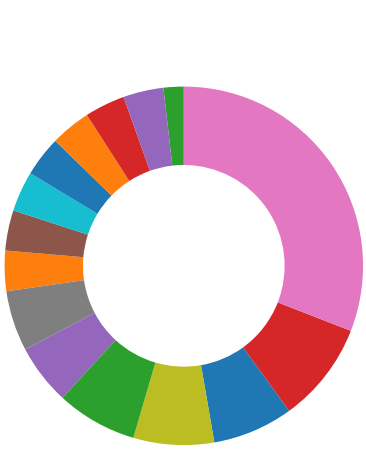
Source	Rule	Description	Author	Strings
3.2.rundll32.exe.3490000.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.2.rundll32.exe.2be0000.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.loaddll32.exe.10000000.4.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.loaddll32.exe.1580000.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.2.rundll32.exe.10000000.5.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud



Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

Yara detected Ursnif

System Summary:

Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

Yara detected Ursnif

Remote Access Functionality:

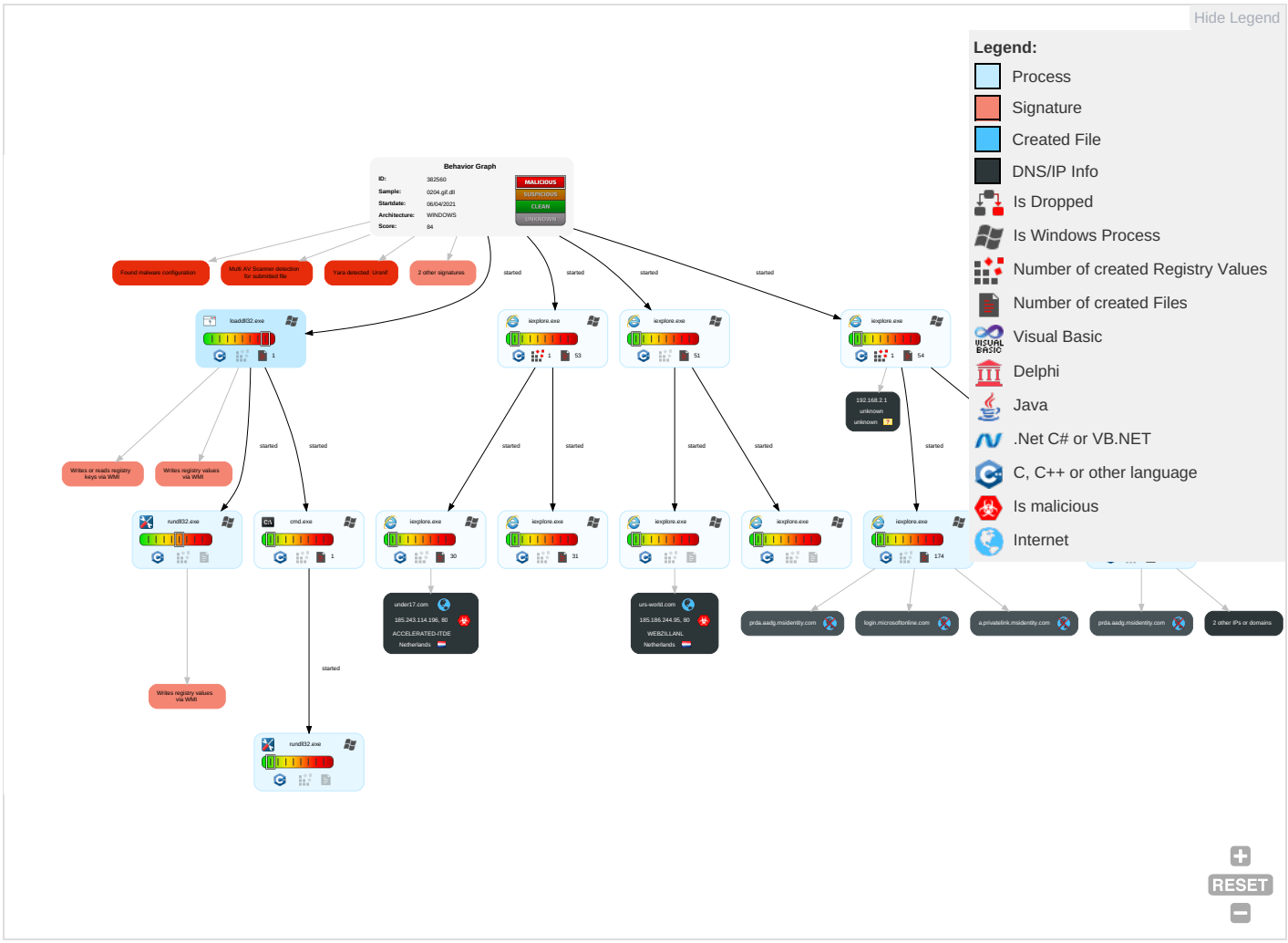
Yara detected Ursnif

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Rem Serv Effe
Valid Accounts	Windows Management Instrumentation 2	Path Interception	Process Injection 1 2	Masquerading 1	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Rem Trac With Auth
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Rem Wipe With Auth
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obta Devi Clou Back
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	

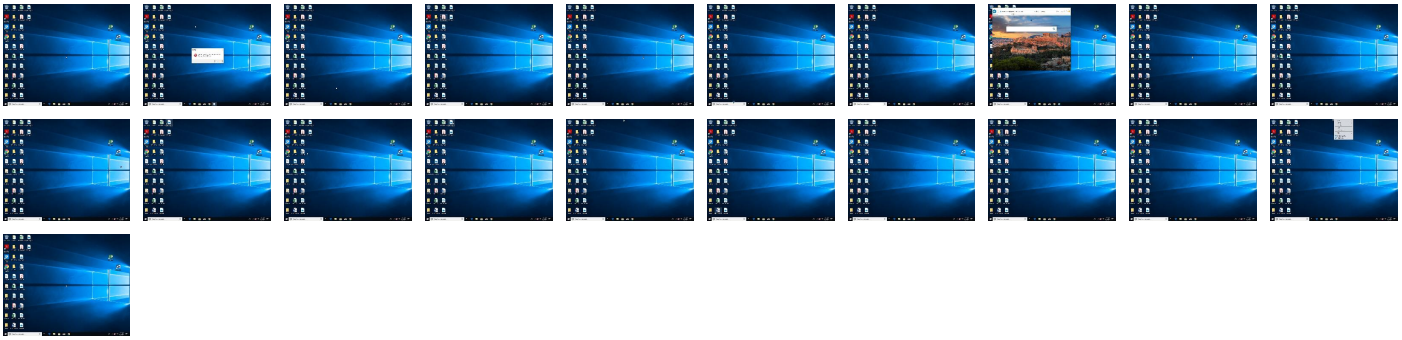
Behavior Graph



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
0204.gif.dll	54%	ReversingLabs	Win32.Trojan.Sdum	
0204.gif.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.3550000.3.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
0.2.loaddll32.exe.1730000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
0.2.loaddll32.exe.10000000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
3.2.rundll32.exe.10000000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://under17.com/joomla/mDD1H_2FL9FujRk_2BcMx/L3jxGl_2F01C5tOn/lz8tvuPEfBFzKF7/SXzkoDSo5ot_2BU2a7/	0%	Avira URL Cloud	safe	
http://under17.com	0%	Avira URL Cloud	safe	
http://under17.com/joomla/FoUDcBGCRMgOiC93_2Fr_/2FiFUTIFAwn6IXco/_2B0KkmSKvezPZ_/2Ftlw1zwyQYlkJ_2BV/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
urs-world.com	185.186.244.95	true	true		unknown
under17.com	185.243.114.196	true	true		unknown
login.microsoftonline.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.msn.com/de-ch/nachrichten/politik/l	msnpopularnow[1].json.22.dr	false		high
http://https://www.msn.com/de-ch/news/other/das-grosse-impfen-beginnt-geht-es-nun-endlich-vorw	msnpopularnow[1].json.22.dr	false		high
http://https://www.msn.com/de-ch/finanzen/top-stories/janet-yellen-us-finanzministerin-fordert-weltweite-mi	msnpopularnow[1].json.22.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/international/so-tickt-kosovos-neue-staatspr	msnpopularnow[1].json.22.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/international/es-h	msnpopularnow[1].json.22.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/vermischtes/die-altersheime-hat-man-vergessen/ar-BB1fkRPW?ocid	msnpopularnow[1].json.22.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/politik/das-alles-h	msnpopularnow[1].json.22.dr	false		high
http://under17.com/joomla/mDD1H_2FL9FujRk_2BcMx/L3jxGl_2F01C5tOn/lz8tvuPEfBFzKF7/SXzkoDSo5ot_2BU2a7/	{10347227-96F9-11EB-90E5-ECF4BB570DC9}.dat.31.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/de-ch/nachrichten/international/alexej-nawalny-klagt-	msnpopularnow[1].json.22.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/politik/manfred-weber-nennt-eu-beitritt-der-t	msnpopularnow[1].json.22.dr	false		high
http://under17.com	loaddll32.exe, 00000000.00000002.498740242.000000000174B000.00000004.00000020.sdmp, rundll32.exe, 00000003.00000002.499825406.0000000003633000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/de-ch/nachrichten/politik/coronakrise-laschet-fordert-harten-br	msnpopularnow[1].json.22.dr	false		high
http://https://www.msn.com/de-ch/news/other/der-westen-muss-mit-sanktionen-drohen-die-wehtun/ar-BB1flkV9?oc	msnpopularnow[1].json.22.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.msn.com/de-ch/news/other/polizei-sucht-mit-superpuma-nach-vermissten-minderj	msnpopularnow[1].json.22.dr	false		high
http://https://www.msn.com/de-ch/finanzen/top-stories/staatliche-regulierung-allianz-gegen-big-tech-druck-a	msnpopularnow[1].json.22.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/politik/fdp-nur-keine-option-von-vornherein-ausschlie	msnpopularnow[1].json.22.dr	false		high
http://under17.com/joomla/FoUDcBGCRMgOiC93_2Fr_/2FiFUTIFAwn6IXco/_2B0KkmSKvezPZ_/2Ftlw1zwyQYlkJ_2BV/	~DF0EA985D0D7E507FA.TMP.31.dr, {10347225-96F9-11EB-90E5-ECF4BB570DC9}.dat.31.dr	false	• Avira URL Cloud: safe	unknown
http://https://login.microsoftonline.com/common/oauth2/authorize?client_id=9ea1ad79-fdb6-4f9a-8bc3-2b70f96e	~DF0D8D159CA42C338F.TMP.20.dr, {F32E7673-96F8-11EB-90E5-ECF4BB570DC9}.dat.20.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/international/ukrainekonflikt-maas-warnt-russland-und-ukraine-	msnpopularnow[1].json.22.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/international/admirale-begehren-auf-gegen-das-verr	msnpopularnow[1].json.22.dr	false		high
http://https://www.msn.com/de-ch/news/other/ressourcen-f	msnpopularnow[1].json.22.dr	false		high
http://https://www.msn.com/de-ch/finanzen/top-stories/datenleck-bei-facebook-wachstum-z	msnpopularnow[1].json.22.dr	false		high
http://https://www.msn.com/de-ch/news/other/auf-schmusekurs-mit-erdogan-eu-spitzen-reisen-in-die-t	msnpopularnow[1].json.22.dr	false		high
http://https://www.msn.com/de-ch/news/other/neuseeland-und-australien-starten-quarant	msnpopularnow[1].json.22.dr	false		high
http://https://www.msn.com/de-ch/news/other/pentagon-usa-beobachten-russlands-aktivit	msnpopularnow[1].json.22.dr	false		high
http://feross.org	GiGr-rA9TBhE2c3LJn7PvDweiOo.gz[1].js.22.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.243.114.196	under17.com	Netherlands		31400	ACCELERATED-ITDE	true
185.186.244.95	urs-world.com	Netherlands		35415	WEBZILLANL	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	382560
Start date:	06.04.2021
Start time:	09:54:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	0204.gif.dll
Cookbook file name:	default.jbs
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:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.troj.winDLL@21/129@8/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 53.2% (good quality ratio 50.7%) • Quality average: 79.8% • Quality standard deviation: 28.3%
HCA Information:	• Successful, ratio: 86% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 20.82.210.154, 93.184.220.29, 131.253.33.200, 13.107.22.200, 92.122.145.220, 184.30.20.56, 13.64.90.137, 40.88.32.150, 88.221.62.148, 20.190.160.73, 20.190.160.71, 20.190.160.2, 20.190.160.6, 20.190.160.69, 20.190.160.129, 20.190.160.8, 20.190.160.134, 20.190.160.67, 20.190.160.136, 20.190.160.4, 52.147.198.201, 20.190.160.132, 92.122.213.194, 92.122.213.247, 52.255.188.83, 205.185.216.42, 205.185.216.10, 152.199.19.161, 20.54.26.129 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, cs9.wac.phicdn.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, www.tm.a.prd.aadg.trafficmanager.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, ocsp.digicert.com, login.live.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, www.tm.a.prd.aadg.akadns.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, www.tm.lg.prod.aadmsa.trafficmanager.net, cs9.wpc.v0cdn.net, store-images.s-microsoft.com-c.edgekey.net, bing.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, go.microsoft.com, arc.trafficmanager.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www2.bing.com, skypedataprdcolwus17.cloudapp.net, ie9comview.vo.msecnd.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, login.msa.msidentity.com, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, www2-bing-com.dual-a-0001.a-msedge.net, go.microsoft.com.edgekey.net, ams2.current.a.prd.aadg.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:55:29	API Interceptor	1x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.243.114.196	gg.gif.dll	Get hash	malicious	Browse	
	gg_1.gif.dll	Get hash	malicious	Browse	
	gg_2.gif.dll	Get hash	malicious	Browse	
	KcFVz0y2si.dll	Get hash	malicious	Browse	
	bTjvWUTLid.dll	Get hash	malicious	Browse	
	KAsJ2r4XYY.dll	Get hash	malicious	Browse	
	swlsGbeQwT.dll	Get hash	malicious	Browse	
	document-1048628209.xls	Get hash	malicious	Browse	
	document-1771131239.xls	Get hash	malicious	Browse	
	document-1370071295.xls	Get hash	malicious	Browse	
	document-69564892.xls	Get hash	malicious	Browse	
	document-1320073816.xls	Get hash	malicious	Browse	
	document-184653858.xls	Get hash	malicious	Browse	
	document-1729033050.xls	Get hash	malicious	Browse	
	document-540475316.xls	Get hash	malicious	Browse	
	document-1456634656.xls	Get hash	malicious	Browse	
	document-1376447212.xls	Get hash	malicious	Browse	
	document-1813856412.xls	Get hash	malicious	Browse	
	document-1776123548.xls	Get hash	malicious	Browse	
	document-684762271.xls	Get hash	malicious	Browse	
185.186.244.95	document-1048628209.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-1771131239.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-69564892.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-1813856412.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-1776123548.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-647734423.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-1579869720.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-806281169.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-839860086.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-1061603179.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-909428158.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-1822768538.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-1952275091.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-583955381.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-1312908141.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-1612462533.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-1669060840.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-203135823.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico
	document-1042699213.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico
	document-980795635.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
urs-world.com	gg.gif.dll	Get hash	malicious	Browse	• 185.186.244.95
	gg_1.gif.dll	Get hash	malicious	Browse	• 185.186.244.95
	gg_2.gif.dll	Get hash	malicious	Browse	• 185.186.244.95
	bTjvWUTLid.dll	Get hash	malicious	Browse	• 185.186.244.95
	KAsJ2r4XYY.dll	Get hash	malicious	Browse	• 185.186.244.95
	swlsGbeQwT.dll	Get hash	malicious	Browse	• 185.186.244.95
	document-1048628209.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1771131239.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-69564892.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1729033050.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1813856412.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1776123548.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-647734423.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1579869720.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-895003104.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-779106205.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-806281169.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-839860086.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1061603179.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-909428158.xls	Get hash	malicious	Browse	• 185.186.244.95
under17.com	gg.gif.dll	Get hash	malicious	Browse	• 185.243.114.196
	gg_1.gif.dll	Get hash	malicious	Browse	• 185.243.114.196
	gg_2.gif.dll	Get hash	malicious	Browse	• 185.243.114.196
	KcFVz0y2si.dll	Get hash	malicious	Browse	• 185.243.114.196
	bTjvWUTLid.dll	Get hash	malicious	Browse	• 185.243.114.196
	KAsJ2r4XYY.dll	Get hash	malicious	Browse	• 185.243.114.196
	swlsGbeQwT.dll	Get hash	malicious	Browse	• 185.243.114.196
	document-1048628209.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1771131239.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1370071295.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-69564892.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1320073816.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-184653858.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1729033050.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-540475316.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1456634656.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1376447212.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1813856412.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1776123548.xls	Get hash	malicious	Browse	• 185.243.114.196

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-684762271.xls	Get hash	malicious	Browse	• 185.243.114.196

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ACCELERATED-ITDE	gg.gif.dll	Get hash	malicious	Browse	• 185.243.114.196
	gg_1.gif.dll	Get hash	malicious	Browse	• 185.243.114.196
	gg_2.gif.dll	Get hash	malicious	Browse	• 185.243.114.196
	KcFVz0y2si.dll	Get hash	malicious	Browse	• 185.243.114.196
	bTjvWUTLid.dll	Get hash	malicious	Browse	• 185.243.114.196
	BnJvVt951o.exe	Get hash	malicious	Browse	• 152.89.236.214
	BnJvVt951o.exe	Get hash	malicious	Browse	• 152.89.236.214
	SMtbg7yHyR.exe	Get hash	malicious	Browse	• 152.89.236.214
	KAsJ2r4XYY.dll	Get hash	malicious	Browse	• 185.243.114.196
	swlsGbeQwT.dll	Get hash	malicious	Browse	• 185.243.114.196
	document-1048628209.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1771131239.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1370071295.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-69564892.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1320073816.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-184653858.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1729033050.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-540475316.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1456634656.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1376447212.xls	Get hash	malicious	Browse	• 185.243.114.196
WEBZILLANL	gg_2.gif.dll	Get hash	malicious	Browse	• 185.186.244.95
	bTjvWUTLid.dll	Get hash	malicious	Browse	• 185.186.244.95
	document-1048628209.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1771131239.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-69564892.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1813856412.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1776123548.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-647734423.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1579869720.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-806281169.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-839860086.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1061603179.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-909428158.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1822768538.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1952275091.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-583955381.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1312908141.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1612462533.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1669060840.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-203135823.xls	Get hash	malicious	Browse	• 185.186.244.95

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{10347223-96F9-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	50344
Entropy (8bit):	2.0005975404985272
Encrypted:	false
SSDEEP:	96:rPZUZi2FW4tAbfgChKMYZqpZQhAlh3t6P43MSUP4OYPwk/YPwOIXLWwnsX/WWI66:rPZUZi2FW4twfgtM9M+jMI+I9sAAItog
MD5:	16D53F13E693A97086E6A89634768E63
SHA1:	A13E958E87E99526A5E5AD97F19F4C4C65008B56
SHA-256:	AAB7C8462B923532FEA54C43F9EF66A20FD9FF81538053A9C32618814624C99D
SHA-512:	E5144D74F16292CBD2994167335DE1A938C56C1AC2DA3C2599BD46A4C0D1571A2EEE9CB2C78DB5864E1947A530A01A4D74B6F658948872D51158692C9F39A66
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{26554461-96F9-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33448
Entropy (8bit):	1.9155600285145717
Encrypted:	false
SSDEEP:	96:rhZ2Zh2MWMt3bfqO1KMCNqdNQmEohEmeV3MlgeVI:rhZ2Zh2MWMtLfqlMn0Q2Mq
MD5:	2F043497C379FA7A3258D32957CC7C77
SHA1:	612D132A20CCE6A7430BCFE7E4C7E3C7AD20D84B
SHA-256:	AE3D6B93C65023823680E02DD7887775507B007AC1C7BCC97B6722597E0B7929
SHA-512:	D39582DB7A34E44E7EC64BE4FCF9BD042BABD089F52BC265D819A97D55414564A18233057459A767856CB689898BCE2190D5BAC1BFB90B5C76609B43135A5E5
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{F32E7671-96F8-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	50344
Entropy (8bit):	1.9999824022145607
Encrypted:	false
SSDEEP:	192:r6ZhZz2HWOtvfVNMFFq/NMUMw8YuHq+ag:rmnK2uH8fq2BwWqS
MD5:	3FE173EC64A5361100EC72F239F5630B
SHA1:	278B7F40F68F29C07D84FF71E46EAD76646BCA36
SHA-256:	F07BF6887063FE6EAD397C43237296738650CC8F0572DE47E518D311A78A5644
SHA-512:	692833753819733 87DAE331CA60808114C9B659F1DA7949830A0AD7CC74020848B408EC0143027E8F3A60226C5B4FE984A93D2DCBD8219242ED5FE0DC727C02C
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{10347225-96F9-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{10347225-96F9-11EB-90E5-ECF4BB570DC9}.dat	
Category:	dropped
Size (bytes):	27380
Entropy (8bit):	1.8465284189029543
Encrypted:	false
SSDEEP:	192:ruZRQt6bkmjF2IWiMSWvPa7SgxvPa7SPPQA:r6mYgg8/TlvPanvPaoPD
MD5:	ABD8A0639358FA57F2E3C8A64CFD0F5D
SHA1:	C1C8CD86DEEB4BBC201817894CC63244BD0011BC
SHA-256:	80CABF00C6C9F67D38955BEB2735116CF9DAB939954B2C68C8BFDAE8BF97693B
SHA-512:	9E4446D035EA4DB8407DB3196FD6D073AA8CED31394D41C914A706F72B58D23927CA315A6963B444CFD3C223EF3E799E29C4E279A1158804D93A1803248FF078
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{10347227-96F9-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	27368
Entropy (8bit):	1.8426399759069807
Encrypted:	false
SSDEEP:	192:r1ZSQY66kOjY24W+MCi6inOlx6inOsinFA:r7/jTlvvXJmx
MD5:	53316A43070A28F35289EBE979D2CEF0
SHA1:	2B6145423BD2B62318069D6C18B28ADE87F6975C
SHA-256:	29DADDE00E2684140CB8AA9A0E474843C5992A030501A89E4E5A2B1FD0A1972C
SHA-512:	FCCB3A2BA788096488057A82D2C2E15D5D1DB288E99330350DBD6F07F7B38E9911236A8E6A76AAB9B36515DCFFCD7340FF0E19514874DAC448D4F61A82258CA
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{26554463-96F9-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.571292948347498
Encrypted:	false
SSDEEP:	48:IwltGcprnmGwpaSG4pQKGrapbS8GQpB6GHHpcrTGUpG:rRZ+Qi68BSUjB2FA
MD5:	9BC70A5AF461833BAF3C3CAE219C7D52
SHA1:	BB7FBACACDD63C563D488708310E7C923CA3F6B1
SHA-256:	0B550D3E6CF3831EE04B46287704E4A0FC35063D150E0C433B893F3A0DD55AD9
SHA-512:	2AFABE7EAA545A10E27377FF337500C0BE48BC5DC5A60E12223A519E4B3DB507751D19819152DAC065A93C0D28CE2316DD200C3AA0AF377A676CF7C8FE48B34
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{26554465-96F9-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5709047515642043
Encrypted:	false
SSDEEP:	48:IwNGcprEGwpaxG4pQNGrapbSLGQpBaGHHpczTGUpG:rTZ8Qj6tBSljh2NA
MD5:	51F7AD841D5EFA9DEF3FFC7A50DF0DE4
SHA1:	51654B4FD92A68DC2029A4A227579BB2463F59F6
SHA-256:	8ED153DC565FEED2C220416B65CF57E2D62686BEECE698EA6C765E9BE9F1E75E
SHA-512:	F4560445138ABD54B58347AF5545CDE43DB52C193DD16E17E77E6D41951C1755102F122DFD2968452395748F85FA4EB4022EAE2246B8790D70072A729BAF95E8
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{26554465-96F9-11EB-90E5-ECF4BB570DC9}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F32E7673-96F8-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	43240
Entropy (8bit):	2.4940213704407586
Encrypted:	false
SSDEEP:	384:r1/9e8nHoi0990EmobffhKfh2DffhZnqX197w:Wh8h2rhB
MD5:	69BB00109B66B48A7AE6DCD2F87FEE83
SHA1:	19DCCB2204AD18862C6EAA2CB341500FABB8E680
SHA-256:	0346AB08C3EA3D91FF4734A50D5367E6E03F4434EEDFF2C3552398B75D5A9749
SHA-512:	5AACE59233F1DE467F3F4BAB387F1D6841FD093B87BE0A0040037901D602ABD813A86B79E23E5F8F27786A165F7440840F49AA09F0BF396AF67830648B449EF5
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F32E7675-96F8-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	43660
Entropy (8bit):	2.538345949708729
Encrypted:	false
SSDEEP:	384:rP3JwXY/0JR6/z7luTfn8fnUAfnvp17jINB:y677luDnmnUSn770L
MD5:	A7AEC1EF23509E9C6AA1690502E76B91
SHA1:	7EBDEE5E7176FD7D481CB03A2369FF1B5679BF22
SHA-256:	7C1610769C0E2A8BB3297F146D304ED561917F9EA64A02536EE4A4A8503B74F5
SHA-512:	A4D2010E544EE10579E42622F028C5B27EB88D5638611B5CE14ACE2EA1E852AAA3594B45CB402DB3078799E08F4C3CA11374E9AE025962F19473E8A4C618AD7
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\dikxvqf\imagestore.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	10192
Entropy (8bit):	4.532955502222545
Encrypted:	false
SSDEEP:	96:0Ph+Qhato4xfDehrmrPh+Qhato4xfDehrm+:0Z+dn5DehKrZ+dn5DehK+
MD5:	BB522C8B17255B17E9094CF89BB841E2
SHA1:	039AB0E66E19AB3C122AD0C9974A28C67148388B
SHA-256:	41CCBE49461865327774763C45CD97B54A94BF3FB457423D89C3337A9FDB429E
SHA-512:	214E9AB26FA26D09BFAFFE45CE4B6A8E487CAE2F2141F10EC4079F610932B87344285C42E9FBA399553CA82744CAE6085E3BB3DEC081F55C764F7713C53C559
Malicious:	false
Preview:	+.h.t.t.p.s.:././.w.w.w...b.i.n.g...c.o.m./.s.a./.s.i.m.g./.f.a.v.i.c.o.n.-.2.x...i.c.o..... ....(... ...@.... ....N...Sz..R...R...P...N..L..H..DG.....R6..U...U...S...R...P...N..L..I..F. .B...7.....S6..V...V...U...S...R...P...N..L..I..F..C...?..:z.....O...W...V...V...U...S...R. ..P...N..L..I..E..C...?...;..{7..q2$.....T..D..]...S)..p6..J...R...P...N..L..I..E..B..>..;..z7..p2..f,X.....A..O#..N!..N! ..N!..P$..q:...P...N..K..I..E..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\4L4QdyjTv0HYE2Ig2ol9eYoqxg8[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1101

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\4L4QdyjTv0HYE2Ig2ol9eYoqxg8[1].svg	
Entropy (8bit):	4.829151166001716
Encrypted:	false
SSDEEP:	24:t0S8eLfl954T0u2y3EO1gRcDrIvQaDxijjfscC:vLfRWtPDuQKljq
MD5:	91CD11CFCCA65CFACE96153268D71F63
SHA1:	E0BE107728D3BF41D8136220DA897D798A2AC60F
SHA-256:	8EE1E6D7A487C38412D7B375AC4A6BD7E47F70858055EEB7957226ADA05544BE
SHA-512:	4367CE147C7FA4590838F23C47819B8954858128336979E28BA116924B92660A7CBDC9A8292C45C5F26FF591F423F03DFADCB78A772DBE86AC5FBABF0B4E7711
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/4L4QdyjTv0HYE2Ig2ol9eYoqxg8.svg
Preview:	<svg focusable="false" width="24px" height="24px" viewBox="0 0 24 24" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">.. <rect fill-opacity="0.2" fill="#000" x="0" y="0" width="24" height="24" rx="2"></rect>.. <g transform="translate(4, 4)">.. <path d="M13.2916881,1.29304814 L7.99 395739,6.59077883 L2.69622669,1.29304814 C2.30349711,0.913737214 1.67923378,0.919161894 1.29315522,1.30524045 C0.907076669,1.691319 0.901651 99,2.31558234 1.28096291,2.70831192 L6.57869361,8.00604261 L1.28096291,13.3037733 C0.90165199,13.6965029 0.907076669,14.3207662 1.29315522,1 4.7068448 C1.67923378,15.0929233 2.30349711,15.098348 2.69622669,14.7190371 L7.99395739,9.42130639 L13.2916881,14.7190371 C13.6844177,15.098348 14.308681,15.0929233 14.6947596,14.7068448 C15.0808381,14.3207662 15.0862628,13.6965029 14.7069519,13.3037733 L9.40922117,8.00604261 L14.7069519,2 .70831192 C15.0976827,2.31746305 15.0976827,1.683897 14.7069519,1.29304814 C14.316103,0.902317288 13

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BJp5dDFvoQm12CHBfp4PC6aiyg4.gz[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	73202
Entropy (8bit):	5.307816444057117
Encrypted:	false
SSDEEP:	1536:kcGJTL/mKzAAFl7JlsG0GRe1cxnoWC1kuyOYkTs/Kun:LGJ4AFl7JlsG0GRCcxnoWC1kuyOYkT0
MD5:	C912DA2683E71660357A600EE34A7873
SHA1:	5DFD028307D4CD8A66492E807B848FEC177AEC3A
SHA-256:	525D57B5D38D8212993C66A33F4CD15EDBD0F260A5AFCF539D092047A908D6EE
SHA-512:	31E2A56C27CC037AD903292DFA518E86642C2A610E9923DD4F7A2FD1347167E042E957A85E98561CC9178318D121DEA3EF165F88EEC79915D0687939DC25BBC
Malicious:	false
Preview:	.scopes{color:rgba(255,255,255,.8);display:inline-block;left:0;white-space:nowrap;list-style:none;line-height:39px}.scopes.sc_hide{display:none}.scopes .scope{font-size:. 8125rem;cursor:pointer;vertical-align:middle;margin-right:36px;background-repeat:no-repeat;position:relative;display:inline-block}.scopes .scope:hover,.scopes .scope.focu sin{color:#fff}.scopes .scope:hover .overflow_menu,.scopes .scope.focusin .overflow_menu{transform:none}.scopes .scope:focus-within .overflow_menu{color:#fff;tr ansform:none}.scopes .scope a{color:inherit;cursor:pointer;text-decoration:none}.scopes .scope.dots{margin-bottom:8px;font-weight:bold}.scopes .scope.dots:befor e{display:inline-block;content:'. . .'}.scopes .scope.dots.hover_focus:focus{outline:none}.scopes .scope .overflow_menu{color:#666;cursor:pointer;transform:scale(0);posit ion:absolute;background-color:#fff;border-radius:6px;padding:4px 0;box-shadow:0 4px 12px 1px rgba(0,0,0,.14);min-width:155px}.scopes .scope .overflow_menu .over flow_item{

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\GiGr-rA9TBhE2c3LJn7PvDweiOo.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	374771
Entropy (8bit):	5.158592433297743
Encrypted:	false
SSDEEP:	6144:1irrzbB3LH7gaV6Z8LAfP0Rp6Izc04YFdNwRm2EjXi4SG7oIBYQmzeH:aHNfi4KwYQmzeH
MD5:	F279A46B56038C41BB3FC11D67D0FE46
SHA1:	B48121E695FD6483CAA7F48DE73FE9F121777109
SHA-256:	A9EA274B393E34591387AC0B4DE594BEE296386543DE34F4897281324DB0DCBB
SHA-512:	4C1754CF5E368D8CE86B135B789A4FF4BAAD1419F30A1EB3B65EAB62217C054D0066EA5FC22B5AA7643EA959854EBC2029B39CB7D1AEAAFB78B95A2A46430F 84
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/GiGr-rA9TBhE2c3LJn7PvDweiOo.gz.js
Preview:	(function(n){function t(r){if(i[r])return i[r].exports;var u=i[r]={i:r,l:!1,exports:{}};return n[r].call(u.exports,u,u.exports,t),u.l=!0,u.exports}var i={};return t.m=n,t.c=i,t.d=function(n, i,r){t.o(n,i)||Object.defineProperty(n,i,{enumerable:!0,get:r})},t.r=function(n){typeof Symbol!="undefined"&&Symbol.toStringTag&&Object.defineProperty(n,Symbol. toStringTag,{value:"Module"});Object.defineProperty(n,"__esModule",{value:!0})},t.t=function(n,i){var r,u;if((i&1&&(n=t(n)),i&8)||i&4&&typeof n=="object"&&n&&n. __esModule)return n;if(r=Object.create(null),t.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:n}),i&2&&typeof n!="string")for(u in n)t.d(r,u,function(t){return n[t]}.bind(null,u));return r},t.n=function(n){var i=n&&n.__esModule?function(){return n["default"]}:function(){return n};return t.d(i,"a",i),i},t.o=function(n,t){return Object.p rototype.hasOwnProperty.call(n,t)},t.p="",t(t.s=0)})([function(n,t,i){window.SpeechSDK=i(1)},function(n,t,i){"use strict";function r(n){for(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\HdepnBaFj-yarvouFUIlfV4Q9D8.gz[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):	3201
Entropy (8bit):	5.369958740257869
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\HdepnBaFj-yarvouFUIlfV4Q9D8.gz[1].js	
SSDEEP:	48:rmo6TIPx85uuYPXznTBB0D6e7htJETfD8QJLxDO7KTUx42Z3rtki:sYuYPXznb0DR7dw8QhIWTQrt7
MD5:	4AADD0F43326BAD8EFD82C85B6D9A20E
SHA1:	4093FC4AB9821B646D64C98051A1CF0679CB2188
SHA-256:	968849A1E6AAED249C78B6CF1AF585AB6C8482A8C5398AB1D2DC3CB92E9EA68F
SHA-512:	616B06A6E3B2385E5487C819FC7F595D473B2F14E8CB76EFB894EDEAB3B26D2C9B679A9B275D924BECC37E156C70B0B56126CCFB62C8B23ABBA9DE07BD93D2A
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/HdepnBaFj-yarvouFUIlfV4Q9D8.gz.js
Preview:	var __spreadArrays=this&&this.__spreadArrays||function(){for(var i=0,n=0,r=arguments.length;n<r;n++)i+=arguments[n].length;for(var u=Array(i),f=0,n=0;n<r;n++)for(var e=arguments[n],t=0,o=e.length;t<o;t++,f++)u[f]=e[t];return u};define("clientinst",["require","exports"],function(n,t){function it(){a=0;u()}function u(){var n,s,t,o;e&&clearTimeout(e);for(n in i)if(i.hasOwnProperty(n)){s=n!=_G.IG?_G.IsUrl.replace(_G.IG,n):_G.IsUrl;for(t in i[n])i[n].hasOwnProperty(t)&&(o=b+s+"&TYPE=Event."+t+"&DATA="+f("[")+i[n][t]+f("]"),ut(o)||(g().src=o));delete i[n]}typeof r!="undefined"&&r.setTimeout&&(e=r.setTimeout(u,w))}function rt(){return _G!==undefined&&_G.EF!==undefined&&_G.EF.logsb!==undefined&&_G.EF.logsb===1}function ut(n){return rt()?ft(n,""):!1}function ft(n,t){var i="sendBeacon",r=!1;if(navigator&&navigator[i])try{navigator[i](n,t);r=!0}catch(u){}return r}var y,d,i,g,o,p;t.__esModule=!0;t.Wrap=t.Log2=t.LogInstrumented=t.Log=t.LogCustomEvent=void 0;var r=n("env"),s=n("event.native"),h=n("e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\Jl2vUSlEIqWjk-99MuYp4W74zvQ[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1529
Entropy (8bit):	4.135964697042234
Encrypted:	false
SSDEEP:	24:tVvnjuJOeUsc4wg5a2/gt+lm/3HljKR99U1TrD3ptYZ7GDlh6ml0jeI4dIwDq8rz:rn1edcjg5pm/lKRXU1TrD5tJf6mzjidJ
MD5:	6D8EF11CB1C03B39D9ED4E4C9A2190B9
SHA1:	265DAF51294422A5A393EF7D32E629E16EF8CEF4
SHA-256:	D72BEAE30A6B2B36C3E03847CE4EA04211D7373D4066FF937A7A05DF4E0C3DB6
SHA-512:	C8820BDF2FC34CCFF7018A1C1E3E74ED1FE0B287926050F9B6BA59C08DCC216E8732F862AB0BF086BC05275C51E6F81132AFA60F6D50A19585642BC906DCDD2
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/Jl2vUSlEIqWjk-99MuYp4W74zvQ.svg
Preview:	<svg width="16" height="16" viewBox="0 0 16 16" fill="none" xmlns="http://www.w3.org/2000/svg">..<path d="M8 0C6.41775 0 4.87103 0.469192 3.55544 1.34824C2.23985 2.22729 1.21447 3.47672 0.608967 4.93853C0.00346629 6.40034 -0.15496 8.00887 0.153721 9.56072C0.462403 11.1126 1.22433 12.538 2.34315 13.6569C3.46197 14.7757 4.88743 15.5376 6.43928 15.8463C7.99113 16.155 9.59966 15.9965 11.0615 15.391C12.5233 14.7855 13.7727 13.7602 14.6518 12.4446C15.5308 11.129 16 9.58225 16 8C16 5.87827 15.1571 3.84344 13.6569 2.34315C12.1566 0.842854 10.1217 0 8 0V0Z" fill="white"/>..<path d="M3.72395 9.60957L5.72394 11.6096C5.97398 11.8595 6.31306 12 6.66661 12C7.02016 12 7.35924 11.8595 7.60928 11.6096L12.2759 6.9429C12.4033 6.81991 12.5049 6.67278 12.5747 6.51011C12.6446 6.34744 12.6814 6.17248 12.6829 5.99544C12.6845 5.8184 12.6507 5.64283 12.5837 5.47897C12.5167 5.3151 12.4177 5.16623 12.2925 5.04104C12.1673 4.91585 12.0184 4.81685 11.8545 4.74981C11.6907 4.68277 11.5151 4.64903 11.3381 4.65057C11.16

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\L4AKO9BL.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):	60829
Entropy (8bit):	5.759786394858774
Encrypted:	false
SSDEEP:	1536:GKrSCXrLQPo3H/8cpUQpqETOuKsIecFXdAjvd894fJLYv6GZob097Q53Opw:GGLQw3f/mQpbd89Riew
MD5:	65DCCDA445D757293B5F409265667D08
SHA1:	1A62F338F5AB13C4D6887EECE38BBF4ED714637A
SHA-256:	A5E86855B6CF58135C849FA06532E8944899A0CF0BE341D3958BCB7046C6C759
SHA-512:	00ACCC709F149F0554425A116E85EF1B7AD478F7E3422BD81CEC9838D2529B608F49935E501E4857414A159D46A7BE3694D34E7812E6C16718AC0D45398A0A01
Malicious:	false
Preview:	<!doctype html><html lang="en" dir="ltr"><head><meta name="theme-color" content="#4F4F4F" /><meta name="description" content="Bing helps you turn information in to action, making it faster and easier to go from searching to doing." /><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta name="viewport" content="width=device-width, initial-scale=1.0" /><meta property="fb:app_id" content="570810223073062" /><meta property="og:type" content="website" /><meta property="og:title" content="Info" /><meta property="og:image" content="https://www.bing.com/th?id=OHR.Olympics125_ROW9889344454_tmb.jpg&rf=" /><meta property="og:image:width" content="1366" /><meta property="og:image:height" content="768" /><meta property="og:url" content="https://www.bing.com/?form=HPFBBK&ssd=20210406_0700&mkt=de-CH" /><meta property="og:site_name" content="Bing" /><meta property="og:description" content="The first modern Olympic Games were held 125 years" /><title>Bing</title><link rel="shortcut i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\MDr1f9aJs4rBVf1F5DAtlALvweY.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	257
Entropy (8bit):	4.781091704776374
Encrypted:	false
SSDEEP:	3:qMH4WXMHwmnIB4JmhyfAIB4Jmml0X2IUJIB4JrNOsK1A4JWW7jKYHVA4JRGYdA4S:q6XzD4jr43ldI74FNQlNj7jM9TlMlbSr
MD5:	51A9EA95D5ED461ED98AC3D23A66AA15

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\MDr1f9aJs4rBVf1F5DAtlALvweY.gz[1].js	
SHA1:	62FBB857B873BD79BEE7F16D0766A452FA2798A3
SHA-256:	A5B4181611E951FAECD6C164D704569C633E95FE68D3D1934B911A089EBF70E8
SHA-512:	CEE4231894F82627E50EC746D7C150E5303A1BF8864D7B084173B9D17663A27CC2915F5D0D4DC0602FE26D9EAA10DD98CF3422E7601F520EF34D45C9A506D6F
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/MDr1f9aJs4rBVf1F5DAtlALvweY.gz.js
Preview:	var BM=BM||{};BM.rules={"#sc_hdu":[-1,-1,1],"#hp_id_hdr":[-1,-1,1],"#hp_container":[-1,-1,1],".hp_sw_logo":[-1,-1,0],".b_searchboxForm":[-1,-1,0],"#crs_pane":[-1,-1,0],"#sb_foot":[-1,-1,0],"#sh_rdiv":[-1,-1,0],"img,div[data-src]":[-1,-1,0],iframe:[-1,-1,0]}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\NGDGShwgz5vCvyjNFyZiaPlHGCE.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	252
Entropy (8bit):	4.837090729138339
Encrypted:	false
SSDEEP:	6:qbLkyK4hImTzBwhLM1whA+XzFE8KSiQLGPQQgnaqza:IQD2IkzaLMGAMzDBVKY+ia
MD5:	1F62E9FDC6CA43F3FC2C4FA56856F368
SHA1:	75ADD74C4E04DB88023404099B9B4AAEA6437AE7
SHA-256:	E1436445696905DF9E8A225930F37015D0EF7160EB9A723BAFC3F9B798365DF6
SHA-512:	6AADAA42E0D86CAD3A44672A57C37ACBA3CB7F85E5104EB68FA44B845C0ED70B3085AA20A504A37DDEDEA7E847F2D53DB18B6455CDA69FB540847CEA6419C DBC
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/NGDGShwgz5vCvyjNFyZiaPlHGCE.gz.js
Preview:	var Button;(function(){WireUp.init("button_init",function(n){var t=n.getAttribute("data-appns"),i=n.getAttribute("data-k");sj_be(n,"click",function(){Log.Log("Click","Button","",!1,"AppNS",t,"K",i,"Category","CommonControls")})})})(Button||(Button={}))

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\QA7QWDV3.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	60359
Entropy (8bit):	5.759693670784069
Encrypted:	false
SSDEEP:	1536:GKrSCXrLQPo3H/8cpUQuqETOuKslecFXdAjvdC94fJLYv8GsOb03Q53O+:GGLQw3f/mQubdC9RPj
MD5:	F09D724372AB360197DB4A73ACD46C85
SHA1:	E5BA6F383E74B4DCBDA6778F5909E7E3C2098AED
SHA-256:	6564DFE91F1D1E3F726BF5D4D8BA69E0C8AEEBDBD26B97AA0BA36DB914CCFDA8
SHA-512:	6CAADCDFD932C2410076740F7933AEF066412065EF387FFE19B69CE8AC46FDBEE91954D7D10D45EA85506079BDB0E9288F89DC40EC48B0C5AEA834CB79DAFE 95
Malicious:	false
IE Cache URL:	http://https://www.bing.com/?form=REDIRERR

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\QA7QWDV3.htm	
Preview:	<!doctype html><html lang="en" dir="ltr"><head><meta name="theme-color" content="#4F4F4F" /><meta name="description" content="Bing helps you turn information in to action, making it faster and easier to go from searching to doing." /><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta name="viewport" content="width=device-width, initial-scale=1.0" /><meta property="fb:app_id" content="570810223073062" /><meta property="og:type" content="website" /><meta property="og:title" content="Info" /><meta property="og:image" content="https://www.bing.com/th?id=OHR.Olympics125_ROW9889344454_tmb.jpg&rf=" /><meta property="og:image:width" content="1366" /><meta property="og:image:height" content="768" /><meta property="og:url" content="https://www.bing.com/?form=HPFBBK&ssd=20210406_0700&mkt=de-CH" /><meta property="og:site_name" content="Bing" /><meta property="og:description" content="The first modern Olympic Games were held 125 years" /><title>Bing</title><link rel="shortcut i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\RXZtj0lYpFm5XDPMpuGSsNG8i9I.gz[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):	1220
Entropy (8bit):	5.024732410536042
Encrypted:	false
SSDEEP:	24:6Vj1V5FrGj6BBEEo6maDU6CWi4dDRRE0Slc7qHy5++vY:8v5TBG6U6C+DLSiL+P
MD5:	E34F2CDADA9986F52CCFAB129645ABAC
SHA1:	93FF6CA74EB48A6825F9BC21BEE52159987C0A82
SHA-256:	79C181E7D29CF735AE99FD86C42934D7FD6FB51E6481D788E1CB812C7DC63DF6
SHA-512:	671EF1DB12BEE74E8E6BAEE8850F4F6A278E51F2236A851A24D889CE40040273088B2D206F2AA42BD1475F4F88F7B4420BC4CE6922023DE205308C56A3C96A4C
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/RXZtj0lYpFm5XDPMpuGSsNG8i9I.gz.js
Preview:	var Feedback;(function(n){var t;(function(){"use strict";function u(t,i){var u=t.getAttribute("id"),f;u||(u="genId"+n.length,t.setAttribute("id",u));f=new r(u,i,t.getAttribute(i));n.push(f)}function i(n,t,i){i===null?n.removeAttribute(t):n.setAttribute(t,i)}function t(n,t,r,f){for(var e,s=_d.querySelectorAll(r),o=0;o<s.length;o++)(e=s[o],f&&e.id&&f[e.id])||(u(e,n),i(e,n,t))}function f(n){for(var u=_d.querySelectorAll(n),e=1,f={},t,i,r=0;r<u.length;++r){if(t=u[r],!t.id){for(;;)if(i="fbpgdgelem"+e++,!_ge(i))break;t.id=i}f[t.id]=t}return f}function e(){var i="tabindex",r="-1",n=f("#fbpgdg, #fbpgdg *");t(i,r,"div",n);t(i,r,"svg",n);t(i,r,"a",n);t(i,r,"li",n);t(i,r,"input",n);t(i,r,"select",n);t("aria-hidden","true","body :not(script):not(style)",n)}function o(){for(var r,t=0;t<n.length;t++)r=_d.getElementById(n[t].id),r&&i(r,n[t].attributeName,n[t].originalAttributeValue);n.length=0}function s(){typeof sj_evt!="undefined"&&(sj_evt.bind("onFeedbackStarting",function(){e()}),sj_evt.bind("onF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\RrvsBuqGHDpqG7NAz4Q0BMOqQBg.gz[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):	4140
Entropy (8bit):	5.268233767834181
Encrypted:	false
SSDEEP:	96:cithlPK4kMRX+1XewlYONYyuGNc22nDmSOsDg:ciJALYONEGNc22nbOsDg
MD5:	7651609B4BE35F5DE8024F570EF6CF87
SHA1:	4B72E4BB1D8F170D6B17FA1D769584A7D0F02F70
SHA-256:	4CA5C607D14D17F8A9EEA9FB0A624BC00C49BFDFBB6A78E1292EAE1461B7D9F0
SHA-512:	7BE114BD02AA079F01FBFC343811F74896BB247ABB79C67998B7DB0F20F8ED1260DEA83523F61CDD0E2231F2428437F9FBF88F39DAD821A3F09A5116C5DA7A2
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/RrvsBuqGHDpqG7NAz4Q0BMOqQBg.gz.js
Preview:	var Feedback;(function(n){var t;(function(){function r(i,r,u,f,e,o){i=typeof i===t?!1:i;i&&scrollTo(0,0);u=typeof u===t?!0:u;n.PackageLoad.Load(r,u,f,e,o)}function e(n,t){for(var r=0,i=null;n&&n.getAttribute&&(!(t>=1)||r<t);){if(i=n.getAttribute("data-fbhlsel"),i!=null)break;r++;n=n.parentNode}return i}var u="feedbackformrequested",c="feedbackInitialized",i,f="",o="feedback-binded",s="clicked",t="undefined",h;n.Bootstrap.InitializeFeedback=function(l,a,v,y,p,w,b,k){function tt(t){var r=null,i;return t&&(i=new h,n.fel("ajax.feedback.collectsettings","gsf",i),r=i.findSettings(t)),r}var d=_ge(a),g,nt;d&&d.classList&&d.classList.contains(o)||(p=typeof p===t?!1:p,g=e(d,3),f!=="sb_feedback"&&(f=a,typeof sj_evt!==t&&(i&&sj_evt.unbind(u,i),i=function(n){var u=null,t=null,f=null,o,i,s;n&&n.length>1&&(i=n[1],i.tagName!==undefined&&i.nodeType!==undefined?(u=i,t=tt(u)):t=i,o=t&&t.elementToHighlight||u,f=e(o));s=t&&t.linkId||a;r(y,l,v,s,f,t)},sj_evt.bind(u,i,1)),typeof SearchAppWrapper!==t&&SearchA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\dnserror[1]	
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(); initMoreInfo('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\4PB7FJMT\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....l..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\favicon-2x[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 32x32, 32 bits/pixel
Category:	dropped
Size (bytes):	4286
Entropy (8bit):	3.8046022951415335
Encrypted:	false
SSDEEP:	24:suZOWcCXPRS4QAUs/KBy3TYI42Apvl6wheXpktCH2Yn4KgISQggggFpz1k9PAYHu:HBRh+sCBykteatiBn4KWi1+Ne
MD5:	DA597791BE3B6E732F0BC8B20E38EE62
SHA1:	1125C45D285C360542027D7554A5C442288974DE
SHA-256:	5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07
SHA-512:	D8DC8358727590A1ED74DC70356AEDC0499552C2DC0CD4F7A01853DD85CEB3AEAD5FBDC7C75D7DA36DB6AF2448CE5ABDFF64CEBDCA3533ECAD953C061A9338E
Malicious:	false
Preview:	....(... ...@..... .....N...Sz..R...R...P...N..L..H..DG.....R6..U...U...S...R...P...N..L..I..F..B...7.....S6..V...V...U...S...R...P...N..L..I..F..C...?...:z.....O...W...V...V...U...S...R...P...N..L..I..E..C...?...:..;..{7..q2$.....T..D..]...S)..p6..J...R...P...N..L..I..E..B..>..;..z7..p2..f,X.....A..O#..N!..N!..N!..P$..q:...P...N..K..I..E..A..=..9..x5..n0..e,...5.....Ea.Z,..T$..T$..T

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\favicon-2x[2].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 32x32, 32 bits/pixel
Category:	downloaded
Size (bytes):	4286
Entropy (8bit):	3.8046022951415335
Encrypted:	false
SSDEEP:	24:suZOWcCXPRS4QAUs/KBy3TYI42Apvl6wheXpktCH2Yn4KgISQggggFpz1k9PAYHu:HBRh+sCBykteatiBn4KWi1+Ne
MD5:	DA597791BE3B6E732F0BC8B20E38EE62
SHA1:	1125C45D285C360542027D7554A5C442288974DE
SHA-256:	5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07
SHA-512:	D8DC8358727590A1ED74DC70356AEDC0499552C2DC0CD4F7A01853DD85CEB3AEAD5FBDC7C75D7DA36DB6AF2448CE5ABDFF64CEBDCA3533ECAD953C061A9338E
Malicious:	false
IE Cache URL:	http://https://www.bing.com/sa/simg/favicon-2x.ico
Preview:	....(... ...@..... .....N...Sz..R...R...P...N..L..H..DG.....R6..U...U...S...R...P...N..L..I..F..B...7.....S6..V...V...U...S...R...P...N..L..I..F..C...?...:z.....O...W...V...V...U...S...R...P...N..L..I..E..C...?...:..;..{7..q2$.....T..D..]...S)..p6..J...R...P...N..L..I..E..B..>..;..z7..p2..f,X.....A..O#..N!..N!..N!..P$..q:...P...N..K..I..E..A..=..9..x5..n0..e,...5.....Ea.Z,..T$..T$..T

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\gDsOfTXNZVl18jxNDvhXqAdf2tM.gz[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):	1821
Entropy (8bit):	5.098212659804913
Encrypted:	false
SSDEEP:	48:0N3GKBel/r5+8cDYC1YvHIH6ayskysb6NccyskpY3Imqc+DkR:oGKBelzw8fCuoaay5ySSy5q3Mc+4R
MD5:	EC15EB7CBFBFAA68BB1DE04A28C80270
SHA1:	D2570D4CFF3139EA66D15799C9E67211F5A03B20
SHA-256:	810A85F1E705231989251F3EB52DAFF3F0ACEE09C703339C301A7CBD22CF8FE6
SHA-512:	077446A676E47447CB771A119CD0EC2EC168E65FED4579E663866D2846F51E93B47367518EB9D79E04EACE139CDFF043E1E28D64559412B4770388B2FEF96A21
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/gDsOfTXNZVl18jxNDvhXqAdf2tM.gz.js
Preview:	(function(){function b(e){var l=e[1],s=l&&_ge(l.vid);s&&(h=_ge("bnp.nid."+f),i=n.getAttribute("data-overlay")==="true"?!0:!1,c=n.getAttribute("data-setscroll")==="true"?!0:!1,k(),ClassUtil.removeClass(h,y),s.style.display="block",c&&d(),sj_evt.fire("bnp.notif.shown",s),i?nt():sj_evt.fire("McpDismissed"),u=_ge(w),t=_ge(v),t.focus(),r=_ge(p),u&&sj_be(u,o,tt),t&&sj_be(t,o,g))}var v="bnp_btn_accept",o="click",y="b_hide",p="cookie_preference",w="bnp_btn_preference",r,u,t,n=_ge("bnp_cookie_banner"),s=_ge("b_footer"),f=_w.bnp.pb_sttc.id,h,e,i,c,k=function(){var t=n&&n.getAttribute("data-position"),i=_ge("bnp_container");i&&t&&t.toLocaleLowerCase()=="top"&&(i.style.top=t+"px",i.style.bottom="auto")},d=function(){var i=_ge("bnp_container"),r=_ge("bnp_action_container"),n=_ge("bnp_content_desc"),u=_ge("bnp_title_container"),t;i&&r&&n&&u&&(t=i.offsetHeight-(r.offsetHeight+u.offsetHeight+130),n.style.maxHeight=t+"px",t<280&&(n.style.marginRight="-10px"))},g=function(t){ManagedCookiePreferenceActio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\lK_FmcR4naKX9hplwfe9ify1hf4.gz[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:	dropped
Size (bytes):	125734
Entropy (8bit):	5.670169400028476
Encrypted:	false
SSDEEP:	1536:ppkCMu1Rv0SuDHT4kfr5IRnO8E9FqJCnq1EoAXycCroA0wT8aHs3:3Mu1Rv0SvNmeGq1ENXdTAVM
MD5:	C24FE194A488B12CCE5B3858D12C2C3D
SHA1:	E55B3E549CA42D614BEE0C4538F9EDA6C89DE00D
SHA-256:	45A1BD96D9A1BB1F03191C2F062FDC5369542864C4777A67623811BE6463D4D6
SHA-512:	4F1C02C2FE716DBEAF061DC9476AD35E33F5C808FD3D79D0ADBECED81B65A02225F7356DBCB10A7232BDD7D02BC0C908F17BB61B058FF5FB99747202522B543
Malicious:	false
Preview:	var __assign=this&&this.__assign||function(){return __assign=Object.assign||function(n){for(var t,r,i=1,u=arguments.length;i<u;i++){t=arguments[i];for(r in t)Object.prototype.hasOwnProperty.call(t,r)&&(n[r]=t[r])}return n},__assign.apply(this,arguments)},__rest=this&&this.__rest||function(n,t){var u={},r;for(var i in n)Object.prototype.hasOwnProperty.call(n,i)&&t.indexOf(i)<0&&(u[i]=n[i]);if(n!=null&&typeof Object.getOwnPropertySymbols=="function")for(r=0,i=Object.getOwnPropertySymbols(n);r<i.length;r++)t.indexOf(i[r])<0&&Object.prototype.propertyIsEnumerable.call(n,i[r])&&(u[i[r]]=n[i[r]]);return u},__spreadArrays=this&&this.__spreadArrays||function(){for(var i=0,n=0,r=arguments.length;n<r;n++)i+=arguments[n].length;for(var u=Array(i),f=0,n=0;n<r;n++)for(var e=arguments[n],t=0,o=e.length;t<o;t++,f++)u[f]=e[t];return u},__awaiter=this&&this.__awaiter||function(n,t,i,r){function u(n){return n instanceof i?n:new i(function(t){t(n)})}return new(i||(i=Promise))(function(i,f){function o(n){

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\msnpopularnow[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	10501
Entropy (8bit):	5.51784121777492
Encrypted:	false
SSDEEP:	192:LUuCIrvL8IgVoZvJZvtctCQwyltHEZdrXgsqBv6SHGjHHAHaBaZvkr1qPUaDQAby:LBCOVmUzaBDePrwsUS/k6Ba52qPJQZEW
MD5:	FC690FA0CC46C5CF583DFBBE141E5A58
SHA1:	E7CCC631BEAE8AC7DC42B1A8259BC752E4938D6F
SHA-256:	8498F9C879FE298FB470D1DB0811F56401425DFBE2388B282C7935FA1E4AC854
SHA-512:	FB1FA394B996687B25D6B05DDC9C77D78538CF281B18E4FD4E797229D68B3C2C692F561AD07B60345078366B2BA27CBFA08B2D2717095D1FBBD0D7159B55959
Malicious:	false
IE Cache URL:	http://https://www.bing.com/hp/api/v1/msnpopularnow?&format=json&ecount=20&efirst=0&&form=REDIRERR
Preview:	{"title":"","data":[{"typeName":"Msn","items":[{"url":"https://www.msn.com/de-ch/news/other/der-westen-muss-mit-sanktionen-drohen-die-wehtun/ar-BB1flkV9?ocid=BingHPC","imageUrl":"/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1flnql.img&ehk=e56b2FA%2fdQ8S1%2bJCLPLA5GewBcl71RQ%2fTmEAxvevKks%3d&w=150&h=150&c=8&rs=2&pid=WP0","shortTitle":"BZ BERNER ZEITUNG","longTitle":"Der Westen muss mit Sanktionen drohen, die wehtun","accessibilityTitle":"","subtext":"","isRecommendedNews":false},{"url":"https://www.msn.com/de-ch/finanzen/top-stories/staatliche-regulierung-allianz-gegen-big-tech-druck-auf-facebook-und-google-w.chst/ar-BB1fkLCT?ocid=BingHPC","imageUrl":"/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkGpp.img&ehk=EoXsvHvTz25OeDlk8%2f1AsQ0JRbPiNyy0iD13c2N9OGI%3d&w=150&h=150&c=8&rs=2&pid=WP0","shortTitle":"Handelsblatt","longTitle":"Staatliche Regulierung: Allianz gegen Big Tech: Druck auf Facebo.","accessibilityTitle":"",""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\n8-O_KIRNSMPFWQWrGjn0BRH6SM.gz[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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\n8-O_KIRNSMPFWQWrGjn0BRH6SM.gz[1].js	
Category:	downloaded
Size (bytes):	1567
Entropy (8bit):	5.248121948925214
Encrypted:	false
SSDEEP:	48:KyskFELvJnSYVtXpQyL93NzpGaQJWA6vrIhf7:KybivJnSE5aU93HGaQJWAilh
MD5:	F9D8B007B765D2D1D4A09779E792FE62
SHA1:	C2CBDA98252249E9E1114D1D48679B493CBFA52D
SHA-256:	9400DF53D61861DF8BCD0F53134DF500D58C02B61E65691F39F82659E780F403
SHA-512:	07032D7D9A55D3EA91F0C34C9CD504700095ED8A47E27269D2DDF5360E4CAC9D0FAD1E6BBFC40B79A3BF89AA00C39683388F690BB5196B40E5D662627A2C49A
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/n8-O_KIRNSMPFWQWrGjn0BRH6SM.gz.js
Preview:	var wln=wln||"",Identity;(function(n){function i(n){n.style.display="none";n.setAttribute("aria-hidden","true")}function r(n){n.style.display="inline-block";n.setAttribute("aria-hidden","false")}var u,t;n&&n.sglid&&sj_be&&sj_cook&&sj_evt&&_d&&typeof _d.querySelectorAll!="undefined"&&(u=function(n){var i=n.getAttribute("data-a"),t=n.getAttribute("data-p");i==="false"&&t!=null&&sj_be(n,"click",function(){sj_cook.set("SRCHUSR","POEX",t,!0,"/")})},sj_evt.bind("identityHeaderShown",function(){var n=!1;sj_be(_ge("id_l"),"click",function(){var i,t;if(!n){for(i=_d.querySelectorAll(".b_imi"),t=0;t<i.length;t++)u(i[t]);n=!0}})},!0));sj_evt&&n&&(t=function(t){var h;if(t==null||t.idp!=="orgid"||(h=n.wlProfile(),h==null||h.name==null||t.name!=null)){var e=_ge("id_n"),u=_ge("id_p"),o=_ge("id_s"),s=_ge("id_a"),f=t?t.displayName:wln,c=t?t.img:null,l=t?t.idp:null,a=t?t.cid:null;e&&s&&(a||f)?(u&&c&&(u.title=f,u.src=c,r(u)),f.length>10&&(f=f.substring(0,10).replace(/\s+$/,"")+"."),e.textContent=f,e.inn

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\ozS3T0fsBUPZy4zlY0UX_e0TUwY.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	226
Entropy (8bit):	4.923112772413901
Encrypted:	false
SSDEEP:	6:2LGfGIEW65JcYCgfkF2/WHRMB58IIR/QxbM76Bhl:2RWIyYCwk4/EMB5ZccbM+B/
MD5:	A5363C37B617D36DFD6D25BFB89CA56B
SHA1:	31682AFCE628850B8CB31FAA8E9C4C5EC9EBB957
SHA-256:	8B4D85985E62C264C03C88B31E68DBABDCC9BD42F40032A43800902261FF373F
SHA-512:	E70F996B09E9FA94BA32F83B7AA348DC3A912146F21F9F7A7B5DEEA0F68CF81723AB4FEDF1BA12B46AA4591758339F752A4EBA11539BEB16E0E34AD7EC946763
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/ozS3T0fsBUPZy4zlY0UX_e0TUwY.gz.js
Preview:	(function(n,t,i){if(t){var r=!1,f=function(){r||(r=!0,typeof wlc!="undefined"&&wlc(sj_evt,sj_cook.set,wlc_t))},u=function(){setTimeout(f,t)};n.bind("onP1",function(){i?n.bind("aad:signedout",u):u()},1)}})(sj_evt,wlc_d,wlc_wfa)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\sTWC0LplwPyIP_jw8VjHps800ZQ.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16386
Entropy (8bit):	5.2866519663601315
Encrypted:	false
SSDEEP:	384:+WLj/9N/zdUjP+c4QQKaK9JASETkyWJLhjO4YuiqRqNlRxW+:+u/P/zdUraOJhaShK1uiqR0T3
MD5:	44AD44162E25A1DB1F46F78B8ECFAD42
SHA1:	C63A0E7B132221D572A541F700601356627A98A4
SHA-256:	5AE500A4737BE7B187EEA99AAB81CF3D4796D23550F7C5349DE2430E6624918D
SHA-512:	4F0078431E86CCD8C0B3DE7E4F7CC10B184DC5376AD10C224EC081DAE1B9D16509E01A95CE3F3B4F7C394EC2C52782E4CB9AC2DE8C12CA0FFC9CC66C01C5AFD
Malicious:	false
Preview:	var customEvents,__spreadArrays,fallbackReplay,EventLoggingModule;_w.EventsToDuplicate=[];_w.useSharedLocalStorage=!1;define("shared",["require","exports"],function(n,t){function s(n,t){for(var r=n.length,i=0;i<r;i++)t(n[i])}function r(n){for(var i=[],t=1;t<arguments.length;t++)i[t-1]=arguments[t];return function(){n.apply(null,i)}}function u(n){i&&event&&(event.returnValue=!1);n&&typeof n.preventDefault=="function"&&n.preventDefault()}function f(n){i&&event&&(event.cancelBubble=!0);n&&typeof n.stopPropagation=="function"&&n.stopPropagation()}function e(n,t,i){for(var r=0;n&&n.offsetParent&&n!=(i||document.body);)r+=n["offset"+t],n=n.offsetParent;return r}function o(){return(new Date).getTime()}function h(n){return i?event:n}function c(n){return i?event?event.srcElement:null:n.target}function l(n){return i?event?event.fromElement:null:n.relatedTarget}function a(n){return i?event?event.toElement:null:n.relatedTarget}function v(n,t,i){while(n&&n!=(i||document.body)){if(n==t)return!0;n=n.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\th[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, 150x150, frames 3
Category:	downloaded
Size (bytes):	4858
Entropy (8bit):	7.912860451432217
Encrypted:	false
SSDEEP:	96:pPE/rJtrOaBegYjEZcV2CWr45p5VrbFU4/PbFI+tMpg:pPYKaBeXE6d59bLui

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\th[1].jpg	
MD5:	C27EAAD7FDCAD067348EB8426A6643DD
SHA1:	D5362D86359F58F1F08EBC9E9F7627F61CB70909
SHA-256:	20EA77BAF0828E450BB7EB0895759B7C760D1F4C00B1EF5366F91B2F23B30429
SHA-512:	AF46A7A9FAEF467FBBA40194C4B8E6A57EDF476ACC10CBEE4CADF87E8CFFA5DBCCB6EC6601944724148F59E8EBCB317442F88BE272657EC4A9EDC841B984F BD2
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkGpp.img&ehk=EoXsvHvTz25OeDlk8%2f1AsQ0JRbPiNyy0iD13c2N9OGI%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....`.`.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=========.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..%8&jP....p..u..p"..z....e.....`.1....:.....J.O3.....k.....6I.J0..1..&K..(P...GS[..b.(."....`zT.....I...3..}g<ig.M.r....~5.....[.....sz.f^.....(^Cg..{...1.....n1.`..A.*.I....m+;Gx.....3..q[..!.p.....G..>VrU.+..).*..iZ.9lU)L)V.SJS$.R.V...2S..J.E...]...sEJR..:5L... ....)..@..s]|i..W..d7.<k.v.=z.....p.=l..,L.].....4...L..c.Q....j..}.%.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\th[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	3889
Entropy (8bit):	7.890192281255403
Encrypted:	false
SSDEEP:	96:5PEjfzwzrOzplwYpimMhIO+Mtm/dZ7a/ve5Suu86PRg2CY/:5P9zizploVKOT0lZO/vCuZPRgc
MD5:	C42031184BC6E5683A2647F391637A4C
SHA1:	45202C0BD8BC0B7835B375DEB9DA76C5658B2F17
SHA-256:	2FCC6397F43A3884B2D1BA97B82A6F269E8B1C9EA8CCB6B072C6124DBD2879D8
SHA-512:	89C84780EE00A098CF9C5839E074FA2B209920E9E9366D7906E30CD017F8350B5D1F72AF67A36A34CACEAF48FD855CDA410E52BA57756BF9D274DFA5E42DC86 F
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1flkPJ.img&ehk=ixnfMu%2bvNEGorqMeHZVbV%2bYB9uGjNgR%2bqRDm083wmkQ%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....H.H.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=========.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..T2X. .+....w*..5zZN..U...x.6.q....?y..sE).....)k.....Q@...4f.....J..Q...Ob..$u:<...._....>:sM...=n.7On;W..i.}\..a.|...R0H..."&h.!..b..m)..D.-..P..Y....dW-..}.....[OSn..n1..q.;.Y".....^e.i..3...I.wKIK^....$0.q .%...2..]?..\....X.1...U.M.i...../.S.....R...<.g3.....~c..7.u.:p\G*.w.....S'x...Q\..I..RBA...z.5.]....Y.,I...L-.t..-.....w.#..@..W.O.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\th[3].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	5777
Entropy (8bit):	7.917920871216737
Encrypted:	false
SSDEEP:	96:pPEQBGjpz1df7dAJrDp5OiC9PchAeKBc9VSwpCcGpZcU1DwGO1pHRsKdDcn:pPTBGjlrf7dNchnrCnZcUwG4Rldon
MD5:	7D10F16EA455E49470853BE05415E27E
SHA1:	0370FE7D24274A9A5909355C042EBBF9E795FD85
SHA-256:	1DB14FB96D4E49265DEFB60E98BD6C39A2724B1EBC21D50E0F2E60F3859EE93A
SHA-512:	DF233159BC504BA5C8D8759AE631A2D5CE9AB48060EDC84EEF2674749AEE1D5E0A3B5BD5AE8EF3F54FDFBBD1F7FE0B9D26FD1FC99593DAC78396EE2209CE1 B0C
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1flksC.img&ehk=H0FCoWHkkRHx9dwEmzqiKOqgx9bfKAuVCxCQfuDoLvw%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....,.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=========.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....;@..^H[~O.=..I.5.s.....8.....%'=..Hd.q..?.W'..... .;..J$...=.E$.P1.h../..7.z.....ZxF.....f1...R.~...i\v!..... .>...u!...9.....\<.I..A....8.....#....-.....h. .|.#tcV..e....1Q.A..W].qV..*..B.i$.z7...Kz.(..l7.#....T?3...o7..H..c(..O..qYF-d.w.\.#.P...y..Hn&~J.S.c5j..6..c....b...N6.L..F.=..M.(.dw..2....f.ce;GC..W*.x|.....*5.....4....v!.c.t 4.+7.9.5".J

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\th[4].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, 150x150, frames 3
Category:	downloaded
Size (bytes):	3726
Entropy (8bit):	7.864083694829938

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\th[4].jpg	
Encrypted:	false
SSDEEP:	48:pyYcuERAB4Zyb8BrwdM18WIaMAVwIIjMC+FrFza8JmQOQYBhvSp/BSq/DVimjw:pPEZc8ROMWWLMcj7rFza8/VY4MsVij
MD5:	A6E6FD3AB66E5A2F49A45CCB2B61B19D
SHA1:	9A7EC1C26991AFC76B694BECB95639DDE2AB9DA2
SHA-256:	8FB3DE41169B7B8547E4F07836C9C9503655B613678E58DE449A0CB65DFACCE4
SHA-512:	278DD1A867D863F595FB3B8398399F5EAFC332FB29981EF4BF9B14DBCBFBC55A9AC2CE3A86EB4A95F6CFC8C8BE9B60FF690BF9AB436D2AD270A3981ED23B45 7B
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkXNm.img&ehk=kxyU8xKPJMs4tMRWRT6cTgj6Bfiij4nG3t8YLJw8HCQ%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....`.`.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)===.. .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....i....Q..@...P.c....8.;..*..\.@.>.....+.:iV.c.0.D.ub.j._..7.G....f.$(..p2....MsN..b..3+tBy>.Z.O.h. .e.O..e....n +._g....p.{....x.f..o,<^...g.\>....7P.* R..#..b0kB..%%tq.....Q@..Q@...u!...(...R.v(..KE.....{....H'.....U,!X.2....K.sa2...p.W8..s...GL...Q./0v.2..$q...q..Gv.....!.r...IU..._U....AYZFn.H^=I=.e..B.+\l4..I.y..p@...j..... A...M.+.v:lG.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\th[5].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	2542
Entropy (8bit):	7.7794956985553245
Encrypted:	false
SSDEEP:	48:5yYcuERATBsC87tpyXKeyzbOZkEPVEGYI0Z8RV8WdxGAia:5PECCC87jyXK7ejRWSRV/dxGva
MD5:	357F88390923FD2D7C54F8EF73A57475
SHA1:	EE6F5D3CBE310AC210CF47D8F1B748B2B0B5205E
SHA-256:	80076FB2A8BD57B72985F5F3557F2B4742DE360994CD05CCA6604653E63404E0
SHA-512:	2AE5C52C81E088CEA10B4240BDF45220AEAC3C4BFDEEC6C098F946BA569AE626E753F7CC116FF133C920C14DBC94083B484A3FA045EC226A32F62D69F85D05 C
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fl5aC.img&ehk=hx9sEjlDgrlxhlQ0dXS9BWLt7M4%2fn9L%2foLPShsm8wa4%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....H.H.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)===.. .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..(...7..(.....d..0..ci.0.H.8.4ow;F..b[ws.....q...r..@...3L_7..?n.....?LV..d?...J+".....)(.....E8.....W.....F,..JZ..Z)(.....J...fv.....@$...0.cn..q.N{g..:...RCp.. 2aG.ll.T..S.....w .9..V...h.E..aE.....(...(..4.J..K../J(N.WB1{..E..l-....(4Q@...[M.0.....18....[..Z.....W.J._.#...;s.q...v.....W.l+kr.-%.#.(...(...(...j`<..:.[.a:QH.WJ1{.....c`.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\th[6].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, 150x150, frames 3
Category:	downloaded
Size (bytes):	5109
Entropy (8bit):	7.913384769447657
Encrypted:	false
SSDEEP:	96:pPELkaw+eKa2pvAJqZbK+VEYjHOxNtlurSUmBjQFr5i8T:pP0kaw+eKXfG+VEYyx1eSUmBI5/T
MD5:	27368154F2C3CF4EDEBC0A95CED35B43
SHA1:	5CAE3ECA10C9A32BC77AF7AEE1E2944590B8BD37
SHA-256:	4406423DC5F852B966777DE5272126839793C96251AB2F063A099C347BE396D9
SHA-512:	8313894648ADD4EF180464FA901403AB911B67A256DE09ACA665D66BA9EAEAE62A67624C3985F3E22BE537E4E8764FD32BD85C06BE7C3CD37A2418FDAD963E(C
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fk2g2.img&ehk=6LEOa661FEfcyTEYPdN22SbtYfGFBqG3UnhDMs6fDjo%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....`.`.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)===.. .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...<V>.....l..y5..t.z.K.Z.o.8.Y....]N.e"^Jv....:.+..$K..m..v.}..v./0R._j.....w.?...=.0.g.E>`..>...P>.Gc]..3.mb=.....Jq..M.H=k.k..B.dg.8.N.....3o .]..*z. P..?.O.9N(...M7i...}..v.}...|..9z+.}.....b;Q..cQZm.7....X...X.....1.c..IIK..k...b3.k.x..N{5q..|.\.:1.5Y.eQ..\.'...&..~.O+..9u.{...a}.....|:.8Z,3.....C..l.....[z..V.-...Q.....x.....Y.g..q....mN.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\5rqGloMo94v3vwNVR5OsxDNd8d0[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\5rqGloMo94v3vwNVR5OsxDNd8d0[1].svg	
Size (bytes):	461
Entropy (8bit):	4.834490109266682
Encrypted:	false
SSDEEP:	6:tI9mc4sl3WGPXN4x7ZguUz/KVqNFvneuFNH2N9wF+tC77LkeWVLKetCsYuwdOvX0:t41WeXNC1f3q/7H2DIZWYeIsrGYyKYx7
MD5:	4E67D347D439EEB1438AA8C0BF671B6B
SHA1:	E6BA86968328F78BF7BF03554793ACC4335DF1DD
SHA-256:	74DEB89D481050FD76A788660674BEA6C2A06B9272D19BC15F4732571502D94A
SHA-512:	BE40E5C7BB0E9F4C1687FFDDBD1FC16F1D2B19B40AB4865BE81DD5CF5F2D8F469E090219A5814B8DAED3E2CD711D4532E648664BFA601D1FF7BBAA83392D30E
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/5rqGloMo94v3vwNVR5OsxDNd8d0.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 32 32"><title>UserSignedOutIcon</title><circle cx="16" cy="16" r="16" fill="#eee"/><path d="M12.73 13.1a3.271 3.271 0 1 1 3.27 3.2 3.237 3.237 0 0 1-3.27-3.2zm-2.73 9.069h1.088a4.91 4.91 0 0 1 9.818 0h1.094a5.884 5.884 0 0 0-3.738-5.434 4.238 4.238 0 0 0 2.1-3.635 4.366 4.366 0 0 0-8.73 0 4.238 4.238 0 0 0 2.1 3.635 5.878 5.878 0 0 0-3.732 5.434z" fill="#666"/><path fill="none" d="M0 0h32v32h-32z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\ELqKWpA6KkapLUFbOLS-IQ2zfXc[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=5, xresolution=74, yresolution=82, resolutionunit=2, software=GIMP 2.10.8, datetime=2019:08:01 11:43:45], progressive, precision 8, 160x160, frames 3
Category:	downloaded
Size (bytes):	9908
Entropy (8bit):	7.8062296698930025
Encrypted:	false
SSDEEP:	192:sWK8UVOGWSkbr43J1ZBpYKL2wth0XM2Cc8AyJKl4xV0KamWtOb+SP0cX:s18bVBrK9B6G2whJ2i/cmygrP0e
MD5:	968C49AC8A1A3EF85F2884F226C55742
SHA1:	10BA8A5A903A2A46A92D415B38B4BE210DB37D77
SHA-256:	E441AFC03F067D1D85DF1F69EB8F482BFDA697CC217E11E1547B3CE964B15B2A
SHA-512:	07B13D6E736683E36091E5BC52F953F9077AD9CD656F0F91E52F17C4630BE3D7524000AA37CFD6CB29ECBB5315F973086630F240118DBE248B4F8A3E79B2B524
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/ELqKWpA6KkapLUFbOLS-IQ2zfXc.jpg
Preview:	......JFIF.....H.H.....PExif..II*.............J..........R...(..........1.......Z...2.......f...z...H.......H.......GIMP 2.10.8.2019:08:01 11:43:45..... .....a.....JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222 22222222....."..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...M.....*.i.@.=h.....)(.....)i(....(.h...)h...ZJZ.(...(...(....(...)i(.....M.N4...S..4..!.E.....(.....(...Z(..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\Fsa_OI0AplCnVoXGca8ALOo0S0s[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	282
Entropy (8bit):	4.768675821769942
Encrypted:	false
SSDEEP:	6:tbXH4mc4sl3UY7eERI1+N9H5R0MLERIwoVNdJMvdIXyCWfuBIAFfu:tbH41niB1+bj0MLBnpavdqyVGBIAFm
MD5:	E38795B634154EC1FF41C6BCDA54EE52
SHA1:	16C6BF388D00A650A75685C671AF002CEA344B4B
SHA-256:	66B589F920473F0FD69C45C8E3C93A95BB456B219CBA3D52873F2A3A1880F3F0
SHA-512:	DCA2E67C46CFF1B9BE39CE8B0D83C34173E6B77EC08FA4EB4BA18A4555144523C570D785549FED7A9909C2E2C3B48D705B6E332832CA4D5DE424B5F7C3CD5BE
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/Fsa_OI0AplCnVoXGca8ALOo0S0s.svg
Preview:	<svg focusable="false" xmlns="http://www.w3.org/2000/svg" viewBox="0 0 16 16">.. <path d="M0 0h16v16h-16z" fill="none"/>.. <path d="M8 1a7 7 0 1 0 7 7 7 7 0 0 0-7-7zm1 10a1 1 0 0 1-2 0v-3a1 1 0 0 1 2 0zm-.293-5.293a1 1 0 1 1 .293-.707 1 1 0 0 1-.293.707z" fill="#767676"/>..</svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\GiGr-rA9TBhE2c3LJn7PvDweiOo.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	206121
Entropy (8bit):	5.13786923319229
Encrypted:	false
SSDEEP:	6144:1irrzbB3LH7gaV6Z8LAfP0Rp6Izc04YFa:aY
MD5:	802D2F0015F148595D5494EAF83F6A2E
SHA1:	B2C6D51F551BAD2060882F4F910A0B12D9FEABE0
SHA-256:	6CEA4B58A1850F3FB6B81470995703A5C01F5C142D3D567128E41813767BD603

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\GiGr-rA9TBhE2c3LJn7PvDweiOo.gz[1].js	
SHA-512:	9EC1D93E2DD416670F895B2F3FACB2F8CA17B72B7B7F29A7D99BE38E5C22B53F4B962DFAD72E0A1B55CBEC3880B436AD4246E6D114CB82614EEEB2012B7750B
Malicious:	false
Preview:	(function(n){function t(r){if(i[r])return i[r].exports;var u=i[r]={i:r,l:!1,exports:{}};return n[r].call(u.exports,u,u.exports,t),u.l=!0,u.exports}var i={};return t.m=n,t.c=i,t.d=function(n,i,r){t.o(n,i)||Object.defineProperty(n,i,{enumerable:!0,get:r})},t.r=function(n){typeof Symbol!="undefined"&&Symbol.toStringTag&&Object.defineProperty(n,Symbol.toStringTag,{value:"Module"});Object.defineProperty(n,"__esModule",{value:!0})},t.t=function(n,i){var r,u;if((i&1&&(n=t(n)),i&8)||i&4&&typeof n=="object"&&n&&n.__esModule)return n;if(r=Object.create(null),t.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:n}),i&2&&typeof n!="string")for(u in n)t.d(r,u,function(t){return n[t]}.bind(null,u));return r},t.n=function(n){var i=n&&n.__esModule?function(){return n["default"]}:function(){return n};return t.d(i,"a",i),i},t.o=function(n,t){return Object.prototype.hasOwnProperty.call(n,t)},t.p="",t(t.s=0)})([function(n,t,i){window.SpeechSDK=i(1)},function(n,t,i){"use strict";function r(n){for(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\PA3TC2iNXZkiG2C3IJp5VAvC_yY.gz[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):	930
Entropy (8bit):	5.191402456846154
Encrypted:	false
SSDEEP:	24:GFUFqJYYmaLOTCE20aOtZP9F3a6MakIq+IvyUJ9sq5aOB:BWOWEZP9U6MHEvyUJ9s6
MD5:	73BFB9BB67A7271E257A4547007469A5
SHA1:	28F7B820679A99318E0DC596A54480D6AD5C3661
SHA-256:	A22BB5BD48C4C578C6BC4FDC4B8FF18F9162848F14E05AE283EC848B08EC8C15
SHA-512:	432142851A492C7635B764AC5293B6EFC943624FBD2FEA5D0F2D8900208B5F6233F5563B7CC08F314E29889B2628F298355484700816A3679F6A3315E63581F0
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/PA3TC2iNXZkiG2C3IJp5VAvC_yY.gz.js
Preview:	var ShareDialog;(function(n){function i(){t("bootstrap",arguments)}function r(){t("show",arguments)}function u(){t("showError",arguments)}function t(n,t){for(var r=["shdlgapi",n],i=0;i<t.length;i++)r.push(t[i]);sj_evt.fire.apply(null,r)}n.bootstrap=i;n.show=r;n.showError=u})(ShareDialog||(ShareDialog={})),function(n){function i(){t==0&&u()}function r(){sj_evt.unbind("shdlgapi",i)}function u(){t=1;var n=ShareDialogConfig.shareDialogUrl+"&IG="+_G.IG;n=e(n,["uncrunched","testhooks"]);sj_ajax(n,{callback:function(n,i){n?(t=2,i.appendTo(_d.body),r(),f()):t=3},timeout:0})}function f(){var n="rms";_w[n]&_w[n].start()}function e(n,t){var i,r,u;for(r in t)u=new RegExp("[?&]"+t[r]+"=[^?&#]*","i"),(i=location.href.match(u))&&i[0]&&(n+="&"+i[0].substring(1));return n}function o(){n.inited=0}function s(){n.inited||(n.inited=1,sj_evt.bind("shdlgapi",i,!0),sj_evt.bind("ajax.unload",o,!1))}var t=0;s()}(ShareDialog||(ShareDialog={}))

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\UYtUYDcn1oZlFG-YfBPz59zejYI[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	964
Entropy (8bit):	4.421237058266115
Encrypted:	false
SSDEEP:	24:t741nTY2jmYXhgauOwgXl3gHuWg9cZLzix9QiVCVCTikxQmQ6Nkpgeoo7:dQnkwXhnuOwIlwHuW7nC9QkaUzQm3Nk5
MD5:	88E3ED3DD7EEE133F73FFB9D36B04B6F
SHA1:	518B54603727D68665146F987C13F3E7DCDE8D82
SHA-256:	A39AB0A67C08D907EDDB18741460399232202C26648D676A22AD06E9C1D874CB
SHA-512:	90FF1284A7FEB9555DFC869644BD5DF8A022AE7873547292D8F6A31BA0808613B6A7F23CB416572ADB298EEE0998E0270B78F41C619D84AB379D0CA9D1D9DA6
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/UYtUYDcn1oZlFG-YfBPz59zejYI.svg
Preview:	<svg focusable="false" xmlns="http://www.w3.org/2000/svg" viewBox="0 0 16 16" enable-background="new 0 0 16 16"><g fill="#00809D"><path d="M2.25 0h-1.25c-.263 0-.521.107-.707.293-.186.186-.293.444-.293.707v1.25c0 .552.448 1 1 1s1-.448 1-1v-.25h.25c.552 0 1-.448 1-1s-.448-1-1-1zM1 8.75c.552 0 1-.448 1-1v-1.5c0-.552-.448-1-1-1s-1 .448-1 1v1.5c0 .552.448 1 1 1zM2.25 12h-.25v-.25c0-.552-.448-1-1-1s-1 .448-1 1v1.25c0 .263.107.521.293.707s.444.293.707.293h1.25c.552 0 1-.448 1-1s-.448-1-1-1zM11.75 2h.25v.25c0 .552.448 1 1 1s1-.448 1-1v-1.25c0-.263-.107-.521-.293-.707-.186-.186-.444-.293-.707-.293h-1.25c-.552 0-1 .448-1 1s.448 1 1 1zM6.25 2h1.5c.552 0 1-.448 1-1s-.448-1-1-1h-1.5c-.552 0-1 .448-1 1s.448 1 1 1zM14.5 7h-.5v-.75c0-.552-.448-1-1-1s-1 .448-1 1v.75h-3.5c-.828 0-1.5.671-1.5 1.5v3.5h-.75c-.552 0-1 .448-1 1s.448 1 1 1h.75v.5c0 .828.672 1.5 1.5 1.5h6c.828 0 1.5-.672 1.5-1.5v-6c0-.829-.672-1.5-1.5-1.5z"/></g><path fill="none" d="M0 0h16v16h-16z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\a282eRIAnHsW_URoyogdzsukm_o.gz[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):	423
Entropy (8bit):	5.117319003552808
Encrypted:	false
SSDEEP:	12:2gSYjthM4GF4aaXtdhI9DfaUZnsMQYAQI:2gSW/bS9/ZnsMAj
MD5:	3A5049DB26AF9CE03DB6A53D3541082D
SHA1:	934DAEA4EDDE2568CA02AB89AF23FDCFEB57339A
SHA-256:	AF8C36DEFED55D79106513865F69933E546E1E4C361E41C29F65905DED009047
SHA-512:	5E21B6E184CBB0013DCCE174345DAC14BB64D391CCA3B253F73C7373253FDCA5E0BB297A0BD2FAD237E4F7968958076606369680621C49C8F99DF428ED3218C9
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/a282eRIAnHsW_URoyogdzsukm_o.gz.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\a282eRIAnHsW_URoyogdzsukm_o.gz[1].js	
Preview:	(function(n){function i(){var e,o,u,s,f,r;if(document.querySelector&&document.querySelectorAll){e=[];o=n.rules;for(u in o)for(s=o[u],u+=!s[2]?"":" >*",f=document.querySelectorAll(u),r=0;r<f.length;r++){var i=f[r],h=0,c=0,l=i.offsetWidth,a=i.offsetHeight;do h+=i.offsetLeft,c+=i.offsetTop;while(i=i.offsetParent);e.push({_e:f[r],x:h,y:c,w:l,h:a})}n.enqueue(t,e)}}var t="L";n.wireup(t,{load:null,compute:i,unload:null})})(BM)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\aL[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gzip compressed data, max speed, from TOPS/20
Category:	dropped
Size (bytes):	393
Entropy (8bit):	7.375865607151121
Encrypted:	false
SSDEEP:	12:XOc0mdh2MN3rO1CTycc42bpHCVad5knR7f2K6Q97X0OTBueaE:XOcBdh2MdrqC/AHCMdAh2utHH
MD5:	2C27746FEF69050D78E1824DCA589C61
SHA1:	DA174FD7AA9822E9A518BEDBE7A1A2DE2127B413
SHA-256:	8D3A29C6D2C9327A508778C6A9E45EA8330A71A4D1D94A918890FF5DC9EA1546
SHA-512:	8732210272AFC3C69BDF723C6740E307BDDCFA2CE7D4AD3756CE6E68800377B0CD09D65E520D5AEFAC34C2A756BFB434E3F33E1BCAE3480D4653A1B20A65F5F9
Malicious:	false
Preview:	.....T.Ko.@...}...+....`..b*...nn..).....LB.__%Yu{...2...hVh*.yK..ih....F...6.....v..2..[.a.f.6.r..8._...y^.....=.V.4....).m....NW.s.k....k}..M.....%N..?..|..".....g..M.....CId.Y.Xbx..C...-Gp....z.w.....1.r...Z.F..3S.x~.....F...."\T.[^J..1.Q.....\.M./pu\.,..=v.6.R.....'.Wgx.m...-.gL..2o.].?.p...-....-.j+X..C...6.J.w...%K4.e.`IV.4F'.B.-U`..x.,..g.....&j.@....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
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
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\B87Z87FM\httpErrorPagesScripts[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):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\lK_FmcR4naKX9hplwfe9ify1hf4.gz[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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\IK_FmcR4naKX9hpIwfe9ify1hf4.gz[1].js	
Category:	downloaded
Size (bytes):	125734
Entropy (8bit):	5.670169400028476
Encrypted:	false
SSDEEP:	1536:ppkCMu1Rv0SuDHT4kfr5IRnO8E9FqJCnq1EoAXycCroA0wT8aHs3:3Mu1Rv0SvNmeGq1ENXdTAVM
MD5:	C24FE194A488B12CCE5B3858D12C2C3D
SHA1:	E55B3E549CA42D614BEE0C4538F9EDA6C89DE00D
SHA-256:	45A1BD96D9A1BB1F03191C2F062FDC5369542864C4777A67623811BE6463D4D6
SHA-512:	4F1C02C2FE716DBEAF061DC9476AD35E33F5C808FD3D79D0ADBECED81B65A02225F7356DBCB10A7232BDD7D02BC0C908F17BB61B058FF5FB99747202522B54 3
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/IK_FmcR4naKX9hpIwfe9ify1hf4.gz.js
Preview:	var __assign=this&&this.__assign||function(){return __assign=Object.assign||function(n){for(var t,r,i=1,u=arguments.length;i<u;i++){t=arguments[i];for(r in t)Object.proto type.hasOwnProperty.call(t,r)&&(n[r]=t[r])}return n},__assign.apply(this,arguments)},__rest=this&&this.__rest||function(n,t){var u={},r;for(var i in n)Object.prototype.ha sOwnProperty.call(n,i)&&t.indexOf(i)<0&&(u[i]=n[i]);if(n!=null&&typeof Object.getOwnPropertySymbols=="function")for(r=0,i=Object.getOwnPropertySymbols(n);r<i.le ngth;r++)t.indexOf(i[r])<0&&Object.prototype.propertyIsEnumerable.call(n,i[r])&&(u[i[r]]=n[i[r]]);return u},__spreadArrays=this&&this.__spreadArrays||function(){for(var i =0,n=0,r=arguments.length;n<r;n++)i+=arguments[n].length;for(var u=Array(i),f=0,n=0;n<r;n++)for(var e=arguments[n],t=0,o=e.length;t<o;t++,f++)u[f]=e[t];return u },__awaiter=this&&this.__awaiter||function(n,t,i,r){function u(n){return n instanceof i?n:new i(function(t){t(n)})}return new(i||(i=Promise))(function(i,f){function o(n){

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\svI82uPNFRD54V4bMLaeahXQXBI.gz[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):	425
Entropy (8bit):	4.963129739598361
Encrypted:	false
SSDEEP:	12:2gXsmzwKN0yApFkRLNF1Jfa1VTWPMg9pIGywV:2gX9zwKN0yAqr1Jfa1V059V
MD5:	016ECFDB34031F881FA5E34DFBD0B7A1
SHA1:	16D3BA1049939D00AE47AAD053993B4762D9B102
SHA-256:	08021ED3BCA5532304B597E636BEB939FF7BAA6D08DCA4E94C0DDE1FDF940389
SHA-512:	D61045D1F07ED241626B8233D388F5E1AD54DBE224871E1CE872ECFD0E29F05A21F0EA02FFDE688FACB134DD969533615493BD35EBA4D5E755840C30A687EE(0
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/svI82uPNFRD54V4bMLaeahXQXBI.gz.js
Preview:	(function(n){function f(){u(sj_be,r)}function r(i){return i&&n.enqueue(t,i),!0}function e(){u(sj_ue,r)}function u(n,t){for(var u,r=0;r<i.length;r++)u=i[r],n(u==="resize"?window:doc ument,window.navigator.pointerEnabled?u.replace("mouse","pointer"):u,t,!1)}var t="EVT",i=["click","mousedown","mouseup","touchstart","touchend","mousemove","tou chmove","scroll","keydown","resize"];n.wireup(t,{load:f,compute:null,unload:e})})(BM)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\swyt_VnIjJDWZW5KEq7a8l_1AEw.gz[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):	2298
Entropy (8bit):	5.34865319631632
Encrypted:	false
SSDEEP:	48:KWEkTScZVcMBOwXhzwBi88RnX8ec0T39B8onA008xG9FLCx3w0S5xJ:KWEkTDZVXpR0BiXjTtB8mA0zxWsx3PG/
MD5:	A8D7D1B3681590980B2D7480906078DB
SHA1:	C9A7A400DB1EBAD4DCA028546EE5F5B2EF4136BD
SHA-256:	1390485DC88B6230389D9C95232A3710BF38D47271708A279B12D7E68E43F649
SHA-512:	710D31EFD76614EC4C94888E2FCC49ABAB50EF406FC0F1C5C10D8AA21D4E9F349DE78068B2BAFE495C074AB4E6EC0A5D44EB5506B2D79C78707A23C1D8206(64
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/swyt_VnIjJDWZW5KEq7a8l_1AEw.gz.js
Preview:	var Bnp=Bnp||{};Bnp.Global=Bnp.Global||{};Bnp.Version="1";Bnp.Partner=Bnp.Partner||function(){function u(n){sj_evt.fire("onBnpRender",n)}function i(n){var r=r||{};if(typeof r.stringify=="function")return r.stringify(n);var o=typeof n,u=n&&n.constructor==Array,f=[],e,t;if(o!="object"||n==null)return o=="string"?""+n+"":String(n);for(e in n)t=n[e], t&&t.constructor!=Function&&(u?f.push(i(t)):f.push(""+e+"":"+i(t)));return(u?"[":"{")+String(f)+(u?"]":"}")}function o(n){for(var r=[],u=n.getElementsByTagName("script") ,t,i;u.length;)t=u[0],i=sj_ce("script"),t.src?i.src=t.src:t.text&&(i.text=t.text),i.type=t.type,t.parentNode.removeChild(t),r.push(i);return r}function s(n){for(var t=0;t<n.length; t++)f(n[t])}function f(n){t=t||_d.getElementsByTagName("head")[0];t.appendChild(n)}function h(n){for(var t,i=0;i<n.length;i++)t=sj_ce("style"),t.type="text/css",t.textCon tent!==undefined?t.textContent=n[i]:t.styleSheet.cssText=n[i],f(t)}function c(){sj_evt.fire("onPopTR")}var n="dhplink",t,e=2500,r=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\th[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 1920x1080, frames 3
Category:	downloaded
Size (bytes):	344983
Entropy (8bit):	7.987666031914428

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\th[1].jpg	
Encrypted:	false
SSDEEP:	6144:uhr6bFSzjuZdOJGR0u6FY7Kq1u9ktnbQ9uJ4g2FUXoIQc1tYJsDr0j:AwFEjSOJbuYphkZQ9uJX22TQc1qJwa
MD5:	DDCE5ED235CCBFFDA3F3735F75F80C0F
SHA1:	F266C24FA6F01459F51C97ADB00523BD214C653C
SHA-256:	78EB4A3213EBE7BB95F87D206AE29064D514628E6A430334D0E13756AA131DE5
SHA-512:	A0C70871BC52467524A0107F09B93C1BE11FFBD9CF68E1F3C567F97B0F810AA5B0CEE584AE1BA720F4A0B30F42E4290A06E99B9EA640437B0DABF158F2DB0625
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?id=OHR.Olympics125_ROW9889344454_1920x1080.jpg&rf=LaDigue_1920x1080.jpg
Preview:	......JFIF.....C..... "" .,,,.3333333333...C..... ....## ##,),,3333333333.....8....".....S..... ....!1A.."Q2aq..B...#R...b.3r....$C.....4Scs..%DT...u.5t.....B.....!..1AQ."aq.2.....BR..#br.$34..C....Ss...c.....?.#...9.%qx..fL.Z..+p.....+...X .2m...,..X.<..W...}Dk.\J....f9.~.....b.../.7C&.V.Y.9`.|.rV0'>.9.....3._>.6.@...ML-...+].Q.....].....'>.`e..W>.9.....|.d...>.9..VJ.Es./.%e....,..y.7.....l.....g.4.3g)..d.99Bk....+r. :e$.ca.SH.|.....m...}.YRO9...j.vd..9V..5..@e...{.<hA...:.....9K#.....q.H...`....q>NiF=.[..2C.8X...*.....L(.{.....s.3.W.!....{^..'..~....9.!..^A.y...1.A..[.....l!a....i ..)L.D.D.8#.{../.0.\.M. .r..qg3...t.N..^....L.I3'.....eQ.`3{.....Yh...sK...k..I...m.o.t^%e...O..e&a.....9..v.x....&.E!.e..p.....n.UQ.x$S\.....1}DqH

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\th[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	4355
Entropy (8bit):	7.900585011984252
Encrypted:	false
SSDEEP:	96:pPE2WJmwonMcP1FpJlLr+clrDFU1Zgk6qe:pPqJfvcPzlpIrDMOk6qe
MD5:	A8AF8B0E212D16641FFF14C692653A31
SHA1:	7F43B7DB65F94F5579B8F338EAEF385F3582573C
SHA-256:	DCA522E3D710326E3009DBEAFD627F940907F615F9922201F636D6352DF50A77
SHA-512:	943633BF7A4E4ABBD086DA138FA68D23A0889CFE815505D641F907241506FB3C9324D6C289F3FE42D86480426F3B8F467AEF1B86626018AD6DC22D47FD1ACF3A
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1flnql.img&ehk=e56b2FA%2fdQ8S1%2bJCLPLA5GewBcI71RQ%2fTmEAxvevKks%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....,.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)===.. .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....H.4.(..J.(..P.....\P.R...p.I.(....ej^%..v.,\L.6.S.....hu}N..X.D=...5..Z.F.....B+%u....E ...U.MN.....<..~.....D.E4...i. ..H....LdDTdT.Tl)...)....O...<.d...(.... . .1KH..ex..[M0El..o%.y.....Z...n.0TE,.z(.$.+{.G....$.G..z6{.9.'b....4.,U.UY.....k&.2...sZP.:g..Z.6.$..J..+'Q....E2....-.....a.^5....*..7.z.cW.bi..n...H..?..Z.S.+1..i.E2F.Q..M1..!".q..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\th[3].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, 150x150, frames 3
Category:	downloaded
Size (bytes):	4987
Entropy (8bit):	7.9205495681055185
Encrypted:	false
SSDEEP:	96:pPE32PK2X6035EzsdUWfNwjh4D8+MhUb80LvFwJp:pPi2PK2Xf35IjWfA4D24LFwH
MD5:	E8349E3EA51D3A6E24284176981359EA
SHA1:	0E009269A3DC197C7C46B765D24AC1F531AA4810
SHA-256:	D88B8253842FB58AADAAEA2166863ADBFF91B77F0CAD8501100A47B7B9A999F6
SHA-512:	85B79D9B4B2C47415EBD2E710EC71B66496F09BDB8822CF8AF7453C3C9D9423869FE3B4DD4D31A89ECFD7E7BC72A55205A306296369F490C12FB05800B6A2A0
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkU9t.img&ehk=mxhBThhQVDlo%2bCYW2VhueyqJguPlSKZ1mWMM3nr17PY%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....`.`.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)===.. .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...i....h..f....E.:.m-..h.74.....I.n.FE...f..I...;4..f.u.<.Bi.....LQLE.Z..U..A.$zS..|8..W(....e.e.F....;F..4.....H..9..;..-q...G.0...]...i....k.....RI.\F.{...G s ...K1..2I8.U;.f.L.....X"iLK'....H..s.....%.H....O..q..G].7.n.$X.pcE...A....k..YS.Kfz8L,+...E+...#....%.D1.....G.+..&.(...\..\.w=C.@.....er.D"h...Fs.J..%.i.s.....:.8. ..i..1.....=k.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\th[4].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	5038
Entropy (8bit):	7.913300499070733
Encrypted:	false
SSDEEP:	96:pPEvzuSDKiT+ERod8yBN0X/HmlRJJ+Fn8h3fzh+LZvwk:pPOCSmHhW/H4JJ+F8xzh+L9wk

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\th[4].jpg	
MD5:	B4253CC44B582EBE891CBCDF0EF5CA8B
SHA1:	2D179CB4C761077F9EFB53625FE0B34D01AE3107
SHA-256:	9358906D6A9154E881A96AA4E9EDED3CCFDF3DC87B1B922B8FC4C09B970130F5
SHA-512:	6D3EA094D383E370E85CBDD445B76D8B2986B3F175145F8DB93112A63E48DF8FA1877BBFD25C2CA73CE66B2C1DECF7FAB01D9556855CF9DD1F9462D4432F60B
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1flcl7.img&ehk=n4zxNzUaGmaWvZYudQOxjiEm8O7nfdAvG5P6LGtz8zo%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....,.,.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)==========.. .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..(...).C$..$gbp..z=.P..`Tz...i.&..+nO._...f7'.....:.....[..zf..a..E.U.(...(...(...(...(.6v.....!..V.k.@.....N...>...Rxc.7:.i.....#.cz..k.4..[i6...bL1c...../.8./.Iob .D+....#,.s..O.I..U7.....z|.i2m.Y...[..j.....Xjodp'HXG..sw>.kJ...Fv2..(..z...D.9L.....b..-./..'....U....t..:}...DV-.u....>u..y...b...Xn.)' ..:.....<>t.e..0...U....=.oN..f...8.(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\th[5].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, 150x150, frames 3
Category:	downloaded
Size (bytes):	3792
Entropy (8bit):	7.879458150606813
Encrypted:	false
SSDEEP:	96:pPEUZavUpaPPjl0qwzhf5Q6u2i7HGLHFgak2bB+u+iiKaCPg8o:pPH0vUWlqhf5Q6uZiDFgak3neaFF
MD5:	E5D2688116BA8D4ABBC53F2493A181BE
SHA1:	2330F5A38AB1DE6979790C84B33DC173F853D6FD
SHA-256:	AA1EF9A296A78952F642406AA0F59930CDD23BC5D1714B7E306787CD4064229E
SHA-512:	0FEBAA0286AFF016B5F0B2B9984D95E2319CA29E41AF624A50D5BF1EDA33CD61017226312DE65B1E5A169A95DB7A6F9212EFFC06A498B0BA857C744CCCBDE3BA
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1flaPv.img&ehk=nfyoU%2b8cc2O%2frjxfHaxiAbz0t%2fXYbGhU6jS%2bwZAdcS0%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....``.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)==========.. .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..x.[.G....uz.....M8.....4..l..2..?..9....$q..r./...LE....'o...w.[H.J..Z..G..Nl.....gC..pk.n..hF.+..<..V...d).....,..Bpj.DT...Rl-..@...i..L.....e.*&(..`...P...l..J... ...@.Mqc}z.....>..)U,y.^.Aq...X...QG.8W....Q..]^..j.|.n~X...[.....\.n.i0..#..9..<Wk.....bx.._.....idb3.A..k7+.....,M./..@...2.?.Y}M....$.....)=....w]....>Y..t+.I....Z.9$.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\th[6].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, 150x150, frames 3
Category:	downloaded
Size (bytes):	4602
Entropy (8bit):	7.919085409507157
Encrypted:	false
SSDEEP:	96:pPEQIac5U07wxonYM7ZCOPHZ3V4DItC+Es/YzbvLSLIBpxrDn5M:pPjeyynnlCoZ32In4TL6CHD+
MD5:	8816AF91855EFB0BB97FAF7429A17E5A
SHA1:	7FFA5A24554D8CA448E6D1F98A7AC31F36CB2FC7
SHA-256:	1C54DB3F6FA0501AB0C6ACC1BFFC8629009F76BE5AA6DE4239FEB24E3C6AEBFC
SHA-512:	F615D37B9E117B9E1A8DC287DC4FD5888BE85F8CB9E9C66E49B547A0D396961177166032251 17D05D7E30734131D15A5C651EFD0B6E9DA546825352B25CCF082
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fjIfk.img&ehk=fogkfx9NpBv%2brwC9WfPL2X5KtkEuDG5AjpDW%2f%2bCifdo%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....``.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)==========.. .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..XqBS.N)..i.,'..H..uH..(..(..5H..$..$...u$...j^/..]4.[...h.).z.V...+.jt1.7E'.).V/.....O...(..c.....8...!ei.|.Y.py...4...=...y_Q.....R{G2Z\4,9'".....7.iz.>..p.. .zP..lz.)....<J.z..P..OZn).H.....h.4P..>(.. S$..J.&.P...(.....e...Py.....mjH...}.#.u..g..@.'.j...v.r.zd..kR..[...$.p.....P.....".b|...9.....8_A.....9.i[J.Y.(#..[.:Ai.<".....k...;d.j:w.\.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\th[7].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, 150x150, frames 3
Category:	downloaded
Size (bytes):	5718
Entropy (8bit):	7.9318718460651025
Encrypted:	false
SSDEEP:	96:pPEJOqsYH47+dCCG6wRGFkXNcO8XOnW81LsImKDFLMwLXZUIEAWgKhE1:pPeOKH470Cv6wRGFSGO8kZ1L8+oiZUrg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\th[7].jpg

MD5:	5ABBBE53C535080AE3BE91FE6F0B93C1
SHA1:	6A991409D0A6886057BBD0DC9AE71AAFB111E8C1
SHA-256:	B692C27DDDA4FFE62BB2C57AA229EB9298EBDA7726BC227089CEEFDF5E05AD4C
SHA-512:	2283634663D24B2C87399A5C562C5E73C68905BF799FD41367D15E4BCF336B5BA5511706998D9C439016799E56B20E5693BCCECA1D9037223D07659410570EC6
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkfuX.img&ehk=Al75D9k%2bIhZGZEnhR9bRctnjlt4TfOCoHOzqmGEyQNE%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....`.`.....C..........................$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C..........=)#)==.. ...."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....?..5..Z...9.{...<....[w..G..W7;..........P.-%V.c..L.>....`A..5.i.".i..A.<.k.....^.Z..u............8.....&.9.I........&..\l.>Ty(.xs...b..........U.*id...r....}zV...Xk>cm.*.[..5.(. u.F......P....;.x....{c..mxfR..........fk....;>..]....[H.u.eO.....4<..C..m.a.....J`..c...z....-.`.B.._.S._....!.......l9.N1...PZ.....z.N...)...M~/.i.p.y.H.b.xP}Y....k......4.X]).l.Fb

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\CMm2G4GK3T9XHTMByeN2QI1OVUs[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=5, xresolution=74, yresolution=82, resolutionunit=2, software=GIMP 2.10.8, datetime=2019:07:31 17:51:08], progressive, precision 8, 160x158, frames 3
Category:	downloaded
Size (bytes):	12415
Entropy (8bit):	7.878337322573188
Encrypted:	false
SSDEEP:	384:dnoYiTiJAAcGIs8E76ZFIN92VPGeBe+ELS:dnyiCAcGIu2FIN92REm
MD5:	A0BFF1A68EAB91DAC459F3B2EB4B3DE3
SHA1:	08C9B61B818ADD3F571D3301C9E376408D4E554B
SHA-256:	7DB453C22084AEF847E1CA04E9FC1B1CF0D468A5C11ABF3C09968C840CD96A87
SHA-512:	3685F5DD0B8869A0B71C4CADF4FE8559094DC431FEE1E14C349BF6E933702B90136EE45277A97627F69BBB6FAB5ED9EF98AFEBCF88079C5EFFEBD4100B64CE21
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/CMm2G4GK3T9XHTMByeN2QI1OVUs.jpg
Preview:	......JFIF.....H.H.....>Exif..II*...............J...........R...(...........1.......Z...2.......f...z...H.......H.......GIMP 2.10.8.2019:07:31 17:51:08.. ..........................P..................JFIF............C.................................. $.' ",#..(7),01444.'9=82<.342...C...........2!.!2222222222222222222222222222222222222222222222222222222..........."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.............................. ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...................... ....?.........,f.iJ..b..vR..6.@...*T..8..0%H...8...cH.I.S.F(.....yZLS.....P..1.,i1F(.s.&.....+..iqR/.(.E.".Q.M)VYiR

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\H_VmuFPRwWZ4UrVl0mPztnf3z5U[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=5, xresolution=74, yresolution=82, resolutionunit=2, software=GIMP 2.10.8, datetime=2019:08:01 11:38:22], progressive, precision 8, 160x160, frames 3
Category:	downloaded
Size (bytes):	13897
Entropy (8bit):	7.900268685598436
Encrypted:	false
SSDEEP:	384:hE9ZTKqcnOdNOEX35wsXK/vWqv/CAU7zXwn1sIQcoo43P:hE9oqcOdfX35wsaWqv6HUn1H4P
MD5:	B545C910F9993F7F930513DB793F4EE0
SHA1:	1FF566B853D1C1667852B565D263F3B677F7CF95
SHA-256:	A797D6446620B867248B43792B9AA457B42ADBB7099D9B3129E0D7743DAF67ED
SHA-512:	12A3A9EC217F8B05151D2BDC76B6B2942C86098F1182AD76B7119B959B9937ACFCACC0361188CDF17A629B1D4E76985DFC6AB409939496AF62354AE9FCEB162
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/H_VmuFPRwWZ4UrVl0mPztnf3z5U.jpg
Preview:	......JFIF.....H.H....!.Exif..II*...............J...........R...(...........1.......Z...2.......f...z...H.......H.......GIMP 2.10.8.2019:08:01 11:38:22.. ....JFIF............C.................................. $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222222222222222222222222222222222222222222.. ...."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....?..-#".Uj..........b.T..Gj.#..E..XD..0...ML...H....i.UN}.p}?:].pE8&O....*q.~UOR@l&...m;...jJE....v..8.p...Z..f'

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\KC_nX2_tPPyFvVw1RK20Yu1FyDk[1].svg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	726
Entropy (8bit):	4.636787858533541
Encrypted:	false
SSDEEP:	12:tbH41nlcWYiB1+Xl0ML2t1iOfEmmgaUEUZQ6nMAIPWSxs4yPISEIe9t8aayPISEx:t741nTYifqLL2+O7mgaxSQ6MFnE3nkO
MD5:	6601E4A25AB847203E1015B32514B16C
SHA1:	282FE75F6FED3CFC85BD5C3544ADB462ED45C839

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\KC_nX2_tPPyFvVw1RK20Yu1FyDk[1].svg	
SHA-256:	6E5D3FFF70EEC85FF6D42C84062076688CB092A3D605F47260DBBE6B3B836B21
SHA-512:	305C325EAD714D7BCBD25F3ACED4D7B6AED6AE58D7D4C2F2DFFCE3DFDEB0F427EC812639AD50708EA08BC79E4FAD8AC2D9562B142E0808936053715938638 7C
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/KC_nX2_tPPyFvVw1RK20Yu1FyDk.svg
Preview:	<svg focusable="false" xmlns="http://www.w3.org/2000/svg" viewBox="0 0 16 16" enable-background="new 0 0 16 16">.. <path d="M0 0h16v16h-16v-16z" fill="none"/>.. <path fill="#007DAA" d="M11 4h4l-5-4v3c0 .552.447 1 1 1zm-3-1v-3h-4.5c-.828 0-1.5.672-1.5 1.5v13c0 .828.672 1.5 1.5 1.5h10c.828 0 1.5-.672 1.5-1.5v-8.5h-4c-1.654 0-3-1.346-3-3zm4.707 10.707c-.181.181-.431.293-.707.293h-7c-.276 0-.526-.112-.707-.293s-.293-.431-.293-.707.112-.526.293-.707.431-.293.707-.293h7c.276 0 .526.112.707.293s.293.431.293.707-.112.526-.293.707zm0-5.414c.181.181.293.431.293.707s-.112.526-.293.707-.431.293-.707.293h-7c-.276 0-.526-.112-.707-.293s-.293-.431-.293-.707.112-.526.293-.707.431-.293.707-.293h7c.276 0 .526.112.707.293z"/>..</svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\Lq2ZTcK-ZOpjsEJIXReQZG4mDLg.gz[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):	67125
Entropy (8bit):	5.23613773666319
Encrypted:	false
SSDEEP:	768:PfY2/W3m6CHbtHgtBkrel21k4Q8BLBSaJBe7BHyJxBCGnVW4nMO51sEBvkH7BSVq:Y2rA3cnq5QPW4nMETv8jYXmNw6V+oF
MD5:	7A6E7F57E8AA30D249A26C481B6CE82C
SHA1:	9902B8665387415875CE0037E4C656F1153D2C
SHA-256:	BAAFA901C91AFC368F4C5443428A247ABE016AD95843AD74148D4321CC0D34DC
SHA-512:	553F287EAEA2583475A96D4F66685C0505FA3961348413F42996631E0F80FC3FF57389EFA6FD5E862F06CAE7110B818BFEED071DF96495CA9EBFB7BCA6FD6162
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/Lq2ZTcK-ZOpjsEJIXReQZG4mDLg.gz.js
Preview:	var AutoSuggest,__extends,Bing,sa_inst;(function(n){var t;(function(n){var t,i,r,u,f,e;(function(n){n.User="SRCHHPGUSR"})(t=n.CookieNames||(n.CookieNames={})),f unction(n){n.AutoSuggest="AS"}(i=n.CrumbNames||(n.CrumbNames={})),function(n){n.CursorPosition="cp";n.ConversationId="cvid";n.SuggestionCount="sc";n.PartialQuer y="pq";n.SuggestionPosition="sp";n.SuggestionType="qs";n.PreviewPaneSuggestionType="qsc";n.SkipValue="sk";n.PreviewPaneSkipValue="skc";n.Ghosting="ghc ";n.Css="css";n.Count="count";n.DataSet="ds";n.SessionId="sid";n.TimeStamp="qt";n.Query="q";n.ImpressionGuid="ig";n.QFQuery="qry";n.BaseQuery="bq";n.F ormCode="form";n.HashedMuid="nclid";n.RequestElToken="elvr";n.ElTokenValue="elv";n.AppId="appid";n.History="history";n.NoHistory="nohs";n.ApiTextDecoration="tex tdecorations";n.ClientId="clientid";n.Market="mkt";n.Scope="scope";n.CountryCode="cc";n.HomeGeographicRegion="hgr";n.SetLang="setlang";n.ZeroInputSerp="zis"}(r= n.QueryParams||(n.QueryParams={})),function(n){n.ImpressionG

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\MstqcgNaYngCBavkktAoSE0--po.gz[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):	391
Entropy (8bit):	5.184440623275194
Encrypted:	false
SSDEEP:	12:2Qxjl/mLAHPWEaaGRHkj6iLUEkFKgs5qHT:2QC8H+aGRHk+i1kFKgs5qHT
MD5:	55EC2297C0CF262C5FA9332F97C1B77A
SHA1:	92640E3D0A7CBE5D47BC8F0F7CC9362E82489D23
SHA-256:	342C3DD52A8A456F53093671D8D91F7AF5B3299D72D60EDB28E4F506368C6467
SHA-512:	D070B9C415298A0F25234D1D7EAFB8BAE0D709590D3C806FCEAEC6631FDA37DFFCA40F785C86C4655AA075522E804B79A7843C647F1E98D97CCE599336DD9D 9
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/MstqcgNaYngCBavkktAoSE0--po.gz.js
Preview:	(function(){function n(){var n=_ge("id_p"),t,i;n&&(t="",i="",n.dataset?(t=n.dataset.src,i=n.dataset.alt):(t=n.getAttribute("data-src"),i=n.getAttribute("data-alt")),t&&t!=""&&(n.on error=function(){n.onerror=null;n.src=" SsJTYQAAAAASUVORK5CYII=";n.alt=""},n.onload=function(){n.alt=i},n.src=t)}n()})()

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\N55Tc-oLNOuzZam9OghLsR0GD5U[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=6, xresolution=86, yresolution=94, resolutionunit=2, software=GIMP 2.10.18, datetime=2020:04:16 19:04:38], progressive, precis ion 8, 160x160, frames 3
Category:	downloaded
Size (bytes):	8245
Entropy (8bit):	7.528284902127932
Encrypted:	false
SSDEEP:	192:BKWN2AtZTviNV8+xq4UZg11u5FR5CUtlkZPRKY:Yi2aZTvNSU+ODR5CCkRr
MD5:	8BC40A6F56CB4477BFB120A472920EC1
SHA1:	379E5373EA0B34EBB365A9BD3A084BB11D060F95
SHA-256:	9050D49D0786F054BC4B7DA42690B034C208A4736B7DE430383A3333A51C9835
SHA-512:	50CD42440CF3C68FC807338C4F5E3AF681FEE41C0767EE7392F9C21A75D2B6483587E89E048128470DBA92EB054E82459BC16A3B0EE61DD89BAEA11E934EAAE 9
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\N55Tc-oLNOuzZam9OghLsR0GD5U[1].jpg	
IE Cache URL:	http://https://www.bing.com/rp/N55Tc-oLNOuzZam9OghLsR0GD5U.jpg
Preview:	......JFIF.....H.H.....Exif..II*.....V.....^...(.....1.....f...2.....t...i.....H.....H.....GIMP 2.10.18..2020:04:16 19:04:38..... .....JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222 22222222222222222222.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz. .....?...(....(...(.....(...(..`.QE..QE..QE..QIH..(...(.....P.E.P.E...QE...QE..-.Q@..R..E.P.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #00 0000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\PA3TC2iNXZkiG2C3IJp5VAvC_yY.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	930
Entropy (8bit):	5.191402456846154
Encrypted:	false
SSDEEP:	24:GFUFqJYYmaLOTCE20aOtZP9F3a6MakIq+IvyUJ9sq5aOB:BWOWEZP9U6MHEvyUJ9s6
MD5:	73BFB9BB67A7271E257A4547007469A5
SHA1:	28F7B820679A99318E0DC596A54480D6AD5C3661
SHA-256:	A22BB5BD48C4C578C6BC4FDC4B8FF18F9162848F14E05AE283EC848B08EC8C15
SHA-512:	432142851A492C7635B764AC5293B6EFC943624FBD2FEA5D0F2D8900208B5F6233F5563B7CC08F314E29889B2628F2983554847008l6A3679F6A3315E63581F0
Malicious:	false
Preview:	var ShareDialog;(function(n){function i(){t("bootstrap",arguments)}function r(){t("show",arguments)}function u(){t("showError",arguments)}function t(n,t){for(var r=["shdl gapi",n],i=0;i<t.length;i++)r.push(t[i]);sj_evt.fire.apply(null,r)}n.bootstrap=i;n.show=r;n.showError=u})(ShareDialog||(ShareDialog={})),function(n){function i(){t==0&&u( )}function r(){sj_evt.unbind("shdlgapi",i)}function u(){t=1;var n=ShareDialogConfig.shareDialogUrl+"&IG="+_G.IG;n=e(n,["uncrunched","testhooks"]);sj_ajax(n,{callback:func tion(n,i){n?(t=2,i.appendTo(_d.body),r(),f()):t=3},timeout:0})}function f(){var n="rms";_w[n]&_w[n].start()}function e(n,t){var i,r,u;for(r in t)u=new RegExp("[?&]"+r+"=[^? &#]*","i"),(i=location.href.match(u))&&i[0]&&(n+="&"+i[0].substring(1));return n}function o(){n.inited=0}function s(){n.inited||(n.inited=1,sj_evt.bind("shdlgapi",i,!0),sj_evt .bind("ajax.unload",o,!1))}var t=0;s()}(ShareDialog||(ShareDialog={}))

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\ULJCe4CXM2DCjZgELMGm2K4PcPo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1642 x 116, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	15917
Entropy (8bit):	7.9392385460477835
Encrypted:	false
SSDEEP:	384:U5vQpWIHNNEojv3nGIsk9MdacywQLntcdejm+sJ/4blz/DXw:Vhl3jj+wcFQLtcMm+K4bR/Dg
MD5:	2D786704B21ADFC7A5037DE337502280
SHA1:	50B2427B80973360C28D98042CC1A6D8AE0F70FA
SHA-256:	54CC8693087FBAF873F72FE9CB4539499A0BC7016225F563DB92B9BFE7EEA564
SHA-512:	625AE0A637BF8B85B86D7719170AAF65ECE69A89CC1E5C76084921A7CABAC226815856D6967403F9264F2C19B4760128C8D10B0FB671D4B9F7A11DBD41B0B6D
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/ULJCe4CXM2DCjZgELMGm2K4PcPo.png
Preview:	.PNG.....IHDR...j...t.....PLTE...uuv.....x.....x.r.....vxzvwywwx.....w.....". .n....uvy.E9...ww{.....x..m.....m.wwy.....l.... tyyuxy.....vxz.m..n....q...m.....{.....vxy///...vv{.m.....twzvvy.....---.....wxz!!!.....3.....vyy...,,.....m.....vvxuu|....L"~.....m..... ....lll."..#.....vwy....Xx,,,....4.....n....vwy....=.....#.....3.....*x.0..3..3..1.....l..$..%.....l.....z..;a.....000.....$.wxz!W.....n....xxx.... .....413....4.....d!..>.....~...Q"qqq....."..www...[[[...Y.....G..)..`.....y..4f.....4....tRNS...0`....`...@_s....A. ...0?....p,.....P?..@...0...~._.aU...o.3.....0.3Q`./y>@ ^B.^.jP.....C.`.....7..nfc.G.... ..88.%...@.....k...).O...M.@....$.d.i....M

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\Xp-HPHGHOZznHBwdn7OWdva404Y.gz[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):	576
Entropy (8bit):	5.192163014367754
Encrypted:	false
SSDEEP:	12:9mPi891gAseP24yXNbdPd1dPkelrR5MdKIKG/OgrfYc3tOfIvHbt:9mPlP5smDy1dV1dHrLMdKIKG/OgLYgtV
MD5:	F5712E664873FDE8EE9044F693CD2DB7
SHA1:	2A30817F3B99E3BE735F4F85BB66DD5EDF6A89F4
SHA-256:	1562669AD323019CDA49A6CF3BDDECE1672282E7275F9D963031B30EA845FFB2
SHA-512:	CA0EB961E52D37CAA75F0F22012C045876A8B1A69DB583FE3232EA6A7787A85BEABC282F104C9FD236DA9A500BA15FDF7BD83C1639BFD73EF8EB6A910B75290D
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/Xp-HPHGHOZznHBwdn7OWdva404Y.gz.js
Preview:	var SsoFrame;(function(n){function t(n){if(n&&n.url&&n.sandbox){var t=sj_ce("iframe"),i=t.style;i.visibility="hidden";i.position="absolute";i.height="0";i.width="0";i.border="none";t.src=decodeURIComponent(n.url);t.id="aadssofr";t.setAttribute("sandbox",n.sandbox);_d.body.appendChild(t);n.currentEpoch&&sj_cook.set("SRCHUSR","T",n.currentEpoch,!0,"/");Log&&Log.Log&&Log.Log("ClientInst","NoSignInAttempt","OrgId",!1)}}function i(n){try{n&&n.length===2&&t(n[1])}catch(i){}}n.createFrame=t;n.ssoFrameEntry=i;sj_evt.bind("ssoFrameExists",i,!0,null,!1)})(SsoFrame||(SsoFrame={}))

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\XvRHqJwJt19aXQca73hQTfvNMxk[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	545
Entropy (8bit):	5.028824557535963
Encrypted:	false
SSDEEP:	12:t4102hriVtBr4pFm9z0kjhlHJW1QOYIX+Xw5RxnnS8K0ML2wtp:t41jiVt5wIz0kjhlHJW1QNCRxS8KLL2a
MD5:	58725E06FABDC207D4350D6F3C5B33D0
SHA1:	5EF447A89C09B75F5A5D071AEF78504DFBCD3319
SHA-256:	EDD5715C42AD596AFE1CF07A400D4F33A2F5388C18ADFDD169A7E9467BC9E9DB
SHA-512:	69F8A2161EDE8AA0BE70ECF641D1C05D7E9B5E6952DD41255E02B7AE9FAFDC94A9547DDDB46A2FF9A56C852239558E3C6634D93A1D6D7669C719956C8D2F5DD6
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/XvRHqJwJt19aXQca73hQTfvNMxk.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 20 20" enable-background="new 0 0 20 20">.. <circle fill="#00809D" cx="10" cy="10" r="3"/>.. <circle fill="#00809D" cx="5.5" cy="5.5" r="1.25"/>.. <path stroke="#00809D" stroke-width="2" stroke-linecap="round" stroke-miterlimit="10" d="M1 7.25v-2.5c0-2.071 1.679-3.75 3.75-3.75h2.5M7.25 19h-2.5c-2.071 0-3.75-1.679-3.75-3.75v-2.5M19 12.75v2.5c0 2.071-1.679 3.75-3.75 3.75h-2.5M12.75 1h2.5c2.071 0 3.75 1.679 3.75 3.75v2.5" fill="none"/>.. <path fill="none" d="M0 0h20v20h-20z"/>..</svg>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\a282eRIAnHsW_URoyogdzsukm_o.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	423
Entropy (8bit):	5.117319003552808
Encrypted:	false
SSDEEP:	12:2gSYjthM4GF4aaXtdhI9DfaUZnsMQYAQI:2gSW/bS9/ZnsMAj
MD5:	3A5049DB26AF9CE03DB6A53D3541082D
SHA1:	934DAEA4EDDE2568CA02AB89AF23FDCFEB57339A
SHA-256:	AF8C36DEFED55D79106513865F69933E546E1E4C361E41C29F65905DED009047
SHA-512:	5E21B6E184CBB0013DCCE174345DAC14BB64D391CCA3B253F73C7373253FDCA5E0BB297A0BD2FAD237E4F796895807660369680621C49C8F99DF428ED3218C9
Malicious:	false
Preview:	(function(n){function i(){var e,o,u,s,f,r;if(document.querySelector&&document.querySelectorAll){e=[];o=n.rules;for(u in o)for(s=o[u],u+=!s[2]?"":" >*",f=document.querySelectorAll(u),r=0;r<f.length;r++){var i=f[r],h=0,c=0,l=i.offsetWidth,a=i.offsetHeight;do h+=i.offsetLeft,c+=i.offsetTop;while(i=i.offsetParent);e.push({_e:f[r],x:h,y:c,w:l,h:a})}n.enqueue(t,e)}}var t="L";n.wireup(t,{load:null,compute:i,unload:null})})(BM)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\b4Jy0kwhnsWcsDQyuzAEsN7RmhQ[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=5, xresolution=74, yresolution=82, resolutionunit=2, software=GIMP 2.10.8, datetime=2019:07:31 17:59:08], progressive, precision 8, 160x160, frames 3
Category:	downloaded
Size (bytes):	14848
Entropy (8bit):	7.9161237402148545
Encrypted:	false
SSDEEP:	192:d5KKqPy60pSDqRxY0cKZR+dG0cDizbS4z0GoJmsrod96rIE1KRCLHXl4DPzEmISD:dg9PJvoe0LsG0liF+TVERCjgEmgDG

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\b4Jy0kwhnsWcsDQyuzAEsN7RmhQ[1].jpg	
MD5:	094FAB391B9B906B8A88922CE6827471
SHA1:	6F8272D24C219EC59CB03432BB3004B0DED19A14
SHA-256:	E7DAFF9BBB32681540E010FB10BA87D51938B42B275D0C422E253CED0DD96B79
SHA-512:	B0BE13E1A3E4B5758DFF4B36C1FF49020565FD316295A7413E5312FB90B0EE4B7D93B4FE4AC5DBB4F122E4CAC0705307A29DA52DBF66A3AC0DA91CC94F5B3EF4
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/b4Jy0kwhnsWcsDQyuzAEsN7RmhQ.jpg
Preview:	......JFIF.....H.H....#JExif..II*.....J.....R...(.....1.....Z...2.....f...z...H.....H.....GIMP 2.10.8.2019:07:31 17:59:08..... .....["....JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222 22222222....."....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....{Ry..J.#..uj..\..\~...f.9..v...M[.....q..Px....(<P.E.P.E.P.J.!8....<.I.T-%F\..Ld.Ff..Sr).....@..M74.i.~.i4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=0
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(); initMoreInfo('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\NUEPGTR9\eRYlUYIMYsB_Pt8B7FTik-pl5cs.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	229
Entropy (8bit):	4.773871204083538
Encrypted:	false
SSDEEP:	3:2LGffIc6CaA5FSAGG4Aj6NhyII6RwZtSAnM+LAX6jUYkjdnwO6yJxWbMPJ/WrE6J:2LGXX6wFSADj6iIunnyh6TbMFsise2
MD5:	EEE26AAC05916E789B25E56157B2C712
SHA1:	5B35C3F44331CC91FC4BAB7D2D710C90E538BC8B
SHA-256:	249BCDCAA655BDEE9D61EDFF9D93544FA343E0C2B4DCA4EC4264AF2CB00216C2
SHA-512:	A664F5A91230C0715758416ADACEEAEFDC9E1A567A20A2331A476A82E08DF7268914DA2F085846A744B073011FD36B1FB47B8E4EED3A0C9F908790439C930538
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/eRYlUYIMYsB_Pt8B7FTik-pl5cs.gz.js
Preview:	(function(){var t=_ge("id_h"),n=_ge("langChange"),i=_ge("me_header"),r=_ge("langDId"),u=_ge("mapContainer");t!=null&&n!=null&&i==null&&(r===null||u===null)&&(t.insertBefore(n,t.firstChild),n.className=n.className+" langdisp")})()

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\eaMqCdNxIXjLc0ATep7tsFkfmSA.gz[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):	2678
Entropy (8bit):	5.2826483006453255
Encrypted:	false
SSDEEP:	48:5sksiMwg1S0h195DlYt/5ZS/wAtKciZIgDa4V8ahSuf/Z/92zBDZDNJC0x0M:yklg1zbed3SBkdZYcZGVFNJCRM
MD5:	270D1E6437F036799637F0E1DFBDCAB5
SHA1:	5EDC39E2B6B1EF946F200282023DEDA21AC22DDE
SHA-256:	783AC9FA4590EB0F713A5BCB1E402A1CB0EE32BB06B3C7558043D9459F47956E
SHA-512:	10A5CE856D909C5C6618DE662DF1C21FA515D8B508938898E4EE64A70B61BE5F219F50917E4605BB57DB6825C925D37F01695A08A01A3C58E5194268B2F4DB3D
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/eaMqCdNxIXjLc0ATep7tsFkfmSA.gz.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\eaMqCdNxIXjLc0ATep7tsFkfmSA.gz[1].js	
Preview:	var IPv6Tests;(function(n){function c(t){var r,c,o,l,f,s,i,a,v;try{if(y(),t==null||t.length==0)return;if(r=sj_cook.get(n.ipv6testcookie,n.ipv6testcrumb),r!=null&&r=="1"&&!u)return;if(c=sj_cook.get(n.ipv6testcookie,n.iptypecrumb),r!=null&&c&&u&&(o=Number(r),l=(new Date).getTime(),o!=NaN&&o>l))return;if(f=_d.getElementsByTagName("head")[0],!f)return;if(s="ipV6TestScript"+t,i=sj_ce("script",s),i.type="text/javascript",i.async=!0,i.onerror=function(){Log.Log("ipv6test","IPv6Test Dom_ "+t,"IPv6TestError",!1,"Error","JSONP call resulted in error.")},a=_ge(s),a&&f)return;f.insertBefore(i,f.firstChild);i.setAttribute("src",_w.location.protocol+"//"+t+".bing.com/ipv6test/test");e&&p();v=u?(new Date).getTime()+h:"1";sj_cook.set(n.ipv6testcookie,n.ipv6testcrumb,v.toString(),!1)}catch(w){Log.Log("ipv6test","Dom_ "+t,"IPv6TestError",!1,"Error","Failed to make JSONP call. Exception - "+w.message)}}function l(t){if(!t){Log.Log("ipv6test","IPv6TestResponseError","IPv6TestError",!1,"Error","Got null re

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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
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\NUEPGTR9\fdVZU4ttbw8NDRm6H3I5BW3_vCo[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	671
Entropy (8bit):	5.014579690661168
Encrypted:	false
SSDEEP:	12:tbH4/KYf3UnlcWYl7qy/gk63xsV8tGXcqecDDWUV8jEPsycd23Wt+MKsAnueOc+d:t74LfEnTYpq+gTxs6GUUQEPssmYsAnuH
MD5:	D9ED1A42342F37695571419070F8E818
SHA1:	7DD559538B6D6F0F0D0D19BA1F7239056DFFBC2A
SHA-256:	0C1E2169110DD2B16F43A9BC2621B78CC55423D769B0716EDAA24F95E8C2E9FE
SHA-512:	67F0BC641D78D5C12671FDD418D541F70517C3CA72C7B4682E7CAC80ABE6730A60D7C3C9778095AAB02C1BA43C8DD4038F48A1A17DA6A5E6C5189B30CA19A15
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/fdVZU4ttbw8NDRm6H3I5BW3_vCo.svg
Preview:	<svg focusable="false" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 16 16" enable-background="new 0 0 16 16" xml:space="preserve">..<path fill="#919191" d="M15.707,0.293c-0.391-0.391-1.024-0.391-1.415,0L7.994,6.591L1.696,0.293C1.298-0.091,0.665-0.08,0.281,0.318...c-0.375,0.388-0.375,1.003,0,1.391l6.298,6.298l-6.298,6.298c-0.384,0.398-0.373,1.031,0.025,1.415c0.388,0.375,1.003,0.375,1.391,0...l6.298-6.298l6.298,6.298c0.398,0.384,1.031,0.373,1.415-0.025c0.375-0.388,0.375-1.003,0-1.39L9.409,8.006l6.298-6.298...C16.098,1.317,16.098,0.684,15.707,0.293z"/>..<path fill="none" d="M0,0h16v16H0V0z"/>..</svg>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\hceflue5sqxkKta9dP3R-IFtPuY.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	426
Entropy (8bit):	4.904019517984965
Encrypted:	false
SSDEEP:	12:2gcmRRt9Y4LF1Zd4XV4LFUXCdg/qUWYzP++xAQI:2gcmRRFfgiUb6MAj
MD5:	857A0DE0BBF14F3427A1AFA5CD985BCE
SHA1:	0C1D2E767F07E5C0F14EA64980DB213D379CC6F7
SHA-256:	3ED65F33193430C0B9DB61FFE7F5FE27B29F86A28563992C3AFC47D4C22C23D7
SHA-512:	E7F2603855A16464417B772517676F080CCEFFB8069C687BAC798B7EB2875FCDC207E40E8C56E7CFFD4D56CED572270988599D1D2B73FB8AAA7FDD076FE3E7E7
Malicious:	false
Preview:	(function(n){function i(){var i=document.documentElement,r=document.body,u="innerWidth"in window?window.innerWidth:i.clientWidth,f="innerHeight"in window?window.innerHeight:i.clientHeight,e=window.pageXOffset||i.scrollLeft,o=window.pageYOffset||i.scrollTop,s=document.visibilityState||"default";n.enqueue(t,{x:e,y:o,w:u,h:f,dw:r.clientWidth,dh:r.clientHeight,v:s})}var t="V";n.wireup(t,{load:null,compute:i,unload:null})})(BM)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\hceflue5sqxkKta9dP3R-IFtPuY.gz[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	426
Entropy (8bit):	4.904019517984965
Encrypted:	false
SSDEEP:	12:2gcmRRt9Y4LF1Zd4XV4LFUXCdg/qUWYzP++xAQI:2gcmRRFfgiUb6MAj
MD5:	857A0DE0BBF14F3427A1AFA5CD985BCE
SHA1:	0C1D2E767F07E5C0F14EA64980DB213D379CC6F7
SHA-256:	3ED65F33193430C0B9DB61FFE7F5FE27B29F86A28563992C3AFC47D4C22C23D7
SHA-512:	E7F2603855A16464417B772517676F080CCEFFB8069C687BAC798B7EB2875FCDC207E40E8C56E7CFFD4D56CED572270988599D1D2B73FB8AAA7FDD076FE3E7E7
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/hceflue5sqxkKta9dP3R-IFtPuY.gz.js
Preview:	(function(n){function i(){var i=document.documentElement,r=document.body,u="innerWidth"in window?window.innerWidth:i.clientWidth,f="innerHeight"in window?window.innerHeight:i.clientHeight,e=window.pageXOffset||i.scrollLeft,o=window.pageYOffset||i.scrollTop,s=document.visibilityState||"default";n.enqueue(t,{x:e,y:o,w:u,h:f,dw:r.clientWidth,dh:r.clientHeight,v:s})}var t="V";n.wireup(t,{load:null,compute:i,unload:null})})(BM)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\hqx6FcD0hjfzrON5oLgx2RMMD1s.gz[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):	443
Entropy (8bit):	4.86644754379557
Encrypted:	false
SSDEEP:	12:kdXCJAUQECJA5MeMJA561cnGfbs4Hbrk86fYXChdJAjU:8CJWECJKMeMJK61cuo47rk8WYMdJyU
MD5:	56583BD882D9571EC02FBDF69D854205
SHA1:	8DFF13B78F4CBCC482DC5C7FC1495390200C0B94
SHA-256:	DF0089A92B304A88F35AA0117CF8647695659AAF68B38B1B7A72A7C53465E9C7
SHA-512:	418B3003B568F2FDB862035EE624CE93087861AEBB6680CDC0E0F1212297B64D30596EEF931B8C6E818292C4AB14C8C17FF0BAF9E58ED93392AD7A80621EBBE
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/hqx6FcD0hjfzrON5oLgx2RMMD1s.gz.js
Preview:	var OutlinePolyfil=function(){function n(){var n=this;this.attachHandlers=function(){n.attachHandlersForOutline()};this.attachHandlersForOutline=function(){addEventListener("keydown",n.onTabKey);addEventListener("mousedown",n.onMouseDown)};this.onTabKey=function(n){n.keyCode==9&&document.body.classList.add("tabbing")};this.onMouseDown=function(){document.body.classList.remove("tabbing")};this.attachHandlers()}return n}();new OutlinePolyfil

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\kBH4DSEA84cgV7IKw7_Bwvm2NpI[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=5, xresolution=74, yresolution=82, resolutionunit=2, software=GIMP 2.10.8, datetime=2019:07:31 17:58:04], progressive, precision 8, 160x160, frames 3
Category:	downloaded
Size (bytes):	11847
Entropy (8bit):	7.82741108986083
Encrypted:	false
SSDEEP:	192:dhK4s5Is9xn1pwLz+SHW36K+Oas6GKNQsjM+N7WzAVrzj+cq615Te+Se:d4ZOOloH/HW3Rp5Ka2tWzAVrzjv55ia
MD5:	5CCC9B225B51915169D6F4C27FA26C9A
SHA1:	9011F80D2100F3872057B20AC3BFC1C2F9B63692
SHA-256:	10D8D2141A01589A82B139B01A75B74D9DFAB16D273C9B2EC7F5087D3EF16B3B
SHA-512:	E2AEB96F6FEC6710AAFF6E52CC24E773CD194F9DEE1BC01FEED88A8EC48033DD9BD8AD0A18C14502DCB6A6ECF05418F18D125E00C4E0E06533495A00F3AF411F
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/kBH4DSEA84cgV7IKw7_Bwvm2NpI.jpg
Preview:	......JFIF.....H.H.....Exif..II*.....J.....R...(.....1.....Z...2.....f...z...H.....H.....GIMP 2.10.8.2019:07:31 17:58:04.....JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222.."}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...LT...{..3....P.1F)....1N....b.S.F(....;.b...\S.F(.....Q..n(.?.b...1O...cqF)....R.1@....b....R.\P.1K.v(. ..\S

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\lK_FmcR4naKX9hpIwfe9ify1hf4.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	50517
Entropy (8bit):	5.612945040100459
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\IK_FmcR4naKX9hpIwfe9ify1hf4.gz[1].js	
SSDEEP:	768:kP5wtNTkCMrK9rQSR4lQlzN6SuDHTzXd2kfrGwIeeK:ppkCMu1Rv0SuDHT4kfr5IRK
MD5:	E3936ED580CC63073DAE11B90D8877A6
SHA1:	4ADD8C29A5A4CC7876DEF37560123A8553CD2508
SHA-256:	8548C80F6F85CA29FAA98B1962AE8CC39CF1436380DC625D6AD25EDF4B3BFA68
SHA-512:	09FC1629EC7BAB8E92A8C7077ED5E171280AD1D4487424422547BA1350EF70EA9676F3BF0859AC267F890CF20BB32BABFA335880DAD5109B3BAA06215CB647A0
Malicious:	false
Preview:	var __assign=this&&this.__assign||function(){return __assign=Object.assign||function(n){for(var t,r,i=1,u=arguments.length;i<u;i++){t=arguments[i];for(r in t)Object.prototype.hasOwnProperty.call(t,r)&&(n[r]=t[r])}return n},__assign.apply(this,arguments)},__rest=this&&this.__rest||function(n,t){var u={},r;for(var i in n)Object.prototype.hasOwnProperty.call(n,i)&&t.indexOf(i)<0&&(u[i]=n[i]);if(n!=null&&typeof Object.getOwnPropertySymbols=="function")for(r=0,i=Object.getOwnPropertySymbols(n);r<i.length;r++)t.indexOf(i[r])<0&&Object.prototype.propertyIsEnumerable.call(n,i[r])&&(u[i[r]]=n[i[r]]);return u},__spreadArrays=this&&this.__spreadArrays||function(){for(var i=0,n=0,r=arguments.length;n<r;n++)i+=arguments[n].length;for(var u=Array(i),f=0,n=0;n<r;n++)for(var e=arguments[n],t=0,o=e.length;t<o;t++,f++)u[f]=e[t];return u},__awaiter=this&&this.__awaiter||function(n,t,i,r){function u(n){return n instanceof i?n:new i(function(t){t(n)})}return new(i||(i=Promise))(function(i,f){function o(n){

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\model[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16168
Entropy (8bit):	5.527579595880806
Encrypted:	false
SSDEEP:	384:HUQyIePm3yt9YYQ5bV5u5hOuKsVMhu3kx0m4iDewY/rfrEraIO1uYPW:0yZ3yjYY85uTOuKsV2u3kx0m4iDewY/i
MD5:	B12C190DFA30C8EF3CACFB2304F8A6BB
SHA1:	4485BA9BCEC741F844120DA43AD4C67EED5EFF0F
SHA-256:	E18575EBB4698CD7418A52E923B8815AA1B288FB160F12A9B8DFE69C816FCA67
SHA-512:	0BE8328FD43826911A8BDD74E85C052F47EA08AF97F36C5C8296648B037C60CFEDA186F81A08C1620728FD50F5D3F36C634CCD2D943C41BEE3DDF3F69515B73
Malicious:	false
Preview:	{"ClientSettings":{"Pn":{"Cn":1,"St":0,"Qs":0,"Prod":"P"},"Sc":{"Cn":1,"St":0,"Qs":0,"Prod":"H"},"Qz":{"Cn":1,"St":0,"Qs":0,"Prod":"T"},"Ap":true,"Mute":true,"Lad":"2021-04-06T00:00:00Z","Iotd":0,"Dft":null,"Mvs":0,"Flt":0,"Imp":2},"MediaContents":[{"ImageContent":{"Description":"The first modern Olympic Games were held 125 years ago in Athens in 1896 . 1,500 years after they were banned by the Roman Emperor. The 1896 Games were held in the Panathenaic Stadium, in the shadow of the Acropolis of Athens, shown here. They included athletes from 14 countries, with the largest delegations from Greece, Germany, France and Great Britain. The 43 events included a marathon, tennis, cycling, fencing, shooting, Greco-Roman wrestling and swimming. And while some things haven't changed over the years, some were different back then. Swimmers were taken out to sea by boat for the longer races and had to swim back to shore. Winners were given a silver medal (copper for second place), as well as an o

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\msnpopularnow[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	10501
Entropy (8bit):	5.51784121777492
Encrypted:	false
SSDEEP:	192:LUuCIrvL8IgVoZvJZvtctCQwyltHEZdrXgsqBv6SHGjHHAHaBaZvkr1qPUaDQAby:LBCOVmUzaBDePrwsUS/k6Ba52qPJQZEW
MD5:	FC690FA0CC46C5CF583DFBBE141E5A58
SHA1:	E7CCC631BEAE8AC7DC42B1A8259BC752E4938D6F
SHA-256:	8498F9C879FE298FB470D1DB0811F56401425DFBE2388B282C7935FA1E4AC854
SHA-512:	FB1FA394B996687B25D6B05DDC9C77D78538CF281B18E4FD4E797229D68B3C2C692F561AD07B60345078366B2BA27CBFA08B2D2717095D1FBBD0D7159B55959
Malicious:	false
Preview:	{"title":"","data":[{"typeName":"Msn","items":[{"url":"https://www.msn.com/de-ch/news/other/der-westen-muss-mit-sanktionen-drohen-die-wehtun/ar-BB1flkV9?ocid=BingHPC","imageUrl":"/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1flnql.img&ehk=e56b2FA%2fdQ8S1%2bJCLPLA5GewBcl71RQ%2fTmEAxvevKks%3d&w=150&h=150&c=8&rs=2&pid=WP0","shortTitle":"BZ BERNER ZEITUNG","longTitle":"Der Westen muss mit Sanktionen drohen, die wehtun","accessibilityTitle":"","subtext":"","isRecommendedNews":false},{"url":"https://www.msn.com/de-ch/finanzen/top-stories/staatliche-regulierung-allianz-gegen-big-tech-druck-auf-facebook-und-google-w.chst/ar-BB1fkLCT?ocid=BingHPC","imageUrl":"/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkGpp.img&ehk=EoXsvHvTz25OeDlk8%2f1AsQ0JRbPiNyy0iD13c2N9OGI%3d&w=150&h=150&c=8&rs=2&pid=WP0","shortTitle":"Handelsblatt","longTitle":"Staatliche Regulierung: Allianz gegen Big Tech: Druck auf Facebo.","accessibilityTitle":"",

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\mw5FvbmnxUiS8Gbwzw9L14Ee8F8.gz[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):	67037
Entropy (8bit):	5.235042447881506
Encrypted:	false
SSDEEP:	768:PfY2/W3m6CHbtHWtBkrel21k4Q8BLBSaJBe7BHyJxBCGnVW4nMO51sEBvkH7BSVq:Y2r23cnq5QPW4nMETv8jYXmNw6V+oF
MD5:	32C8A14D92DE1A36A11B131D48E4C307
SHA1:	5498735530EE16C300CB9E1691BA7356D3163BAC
SHA-256:	CCB7262C883581BB88476377D29E45FE415A403B5DB1143EE493166EF3E2D047
SHA-512:	775BCF9C00D56A28840D30172CC2D598412475FFC5D169F83041AF25C17C5EE252F7B7E272362876ABA83CEC34C9752634663D90502B3F75CF31113283E53A3E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\mw5FvbmnxUiS8Gbwzw9L14Ee8F8.gz[1].js	
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/mw5FvbmnxUiS8Gbwzw9L14Ee8F8.gz.js
Preview:	var AutoSuggest,__extends,Bing,sa_inst;(function(n){var t;(function(n){var t,i,r,u,f,e;(function(n){n.User="SRCHHPGUSR"})(t=n.CookieNames||(n.CookieNames={})),function(n){n.AutoSuggest="AS"}(i=n.CrumbNames||(n.CrumbNames={})),function(n){n.CursorPosition="cp";n.ConversationId="cvid";n.SuggestionCount="sc";n.PartialQuery="pq";n.SuggestionPosition="sp";n.SuggestionType="qs";n.PreviewPaneSuggestionType="qsc";n.SkipValue="sk";n.PreviewPaneSkipValue="skc";n.Ghosting="ghc";n.Css="css";n.Count="count";n.DataSet="ds";n.SessionId="sid";n.TimeStamp="qt";n.Query="q";n.ImpressionGuid="ig";n.QFQuery="qry";n.BaseQuery="bq";n.FormCode="form";n.HashedMuid="nclid";n.RequestElToken="elvr";n.ElTokenValue="elv";n.AppId="appid";n.History="history";n.NoHistory="nohs";n.ApiTextDecoration="textdecorations";n.ClientId="clientid";n.Market="mkt";n.Scope="scope";n.CountryCode="cc";n.HomeGeographicRegion="hgr";n.SetLang="setlang";n.ZeroInputSerp="zis"}(r=n.QueryParams||(n.QueryParams={})),function(n){n.ImpressionG

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\n1U5gwBiwMo7s-fWOh2kSe3Kils[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=5, xresolution=74, yresolution=82, resolutionunit=2, software=GIMP 2.10.8, datetime=2019:07:31 17:53:43], progressive, precision 8, 160x160, frames 3
Category:	downloaded
Size (bytes):	12094
Entropy (8bit):	7.886865463015066
Encrypted:	false
SSDEEP:	192:SiKi8QXz83TatNZ7rBakT+m47amRNj5y4zYOyuRHExmmjGjWddkuz4nicyktAtmR:SRi8083g7rBamzWNjPzguCxmmjGid60g
MD5:	05034EB84E5E7915CA36EB6FE59DFBA7
SHA1:	9F5539830062C0CA3BB3E7D63A1DA449EDCA8A5B
SHA-256:	9BEC2E05752C0699DB84352BB6E3DD4E5DAA927D32EC8123966F4A8FDF8B181A
SHA-512:	EB645D1FBB404B00D19C743C3F6F00597D91DE73EA2F02AE61AB76AFB13A913F68CB2419C205684CAD827D1369D8F76D9B7E709B8EF0AB05A86B305A7A5B708 9
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/n1U5gwBiwMo7s-fWOh2kSe3Kils.jpg
Preview:	.....JFIF.....H.H.....zExif..II*.....J.....R...(.....1.....Z...2.....f...z...H.....H.....GIMP 2.10.8.2019:07:31 17:53:43..... .....JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222.. ....."....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..8...R.Vf.|lcR.....sJ.#...1+..VR:b.b....8&*B.Qq.fj.6W50....`L.z..OrK_.+v..+..2....1.Q...K!.b..n.).A.j.s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\n_C4vBfAV3O9RfkGjfduaZoxjAs[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=5, xresolution=74, yresolution=82, resolutionunit=2, software=GIMP 2.10.8, datetime=2019:08:01 11:40:12], progressive, precision 8, 160x160, frames 3
Category:	downloaded
Size (bytes):	17171
Entropy (8bit):	7.923606790170532
Encrypted:	false
SSDEEP:	384:oYOT4bsa8uRaCLYIrdjf7xR346jojxR0WKHfoe:oYOT4Ya8uRnxT/346AhKHfoe
MD5:	D7AE018EA70FA15F5E5389E4F96AD768
SHA1:	9FF0B8BC17C05773BD45F9068DF76E699A318C0B
SHA-256:	A4F4A44961E03A073E3F351F296EC19C50005AA96360A9E5CEE50E0587738FBB
SHA-512:	FD5B341BECCBBE7C16065217BBCAF6DF2C44629DE778E1263FE6A071565718C920335DBA220FDDF8EB18ECBBF2BEBC698B03BCF555949CB3DD665752494714 06
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/n_C4vBfAV3O9RfkGjfduaZoxjAs.jpg
Preview:	.....JFIF.....H.H....(.Exif..II*.....J.....R...(.....1.....Z...2.....f...z...H.....H.....GIMP 2.10.8.2019:08:01 11:40:12..... .....(.....JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222.. ....."....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...3J8...D....m8P...\.L..c..%.4.R...@.iqJ.4.CCJ.o.....-.!...1.Q.LB...S.U~...iXw.1J(..b.o.b.zSsHb.@..(... .H:...M.O4.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\pXscrbCrewUD-UetJTvW5F7YMxo.gz[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):	511
Entropy (8bit):	4.980041296618112
Encrypted:	false
SSDEEP:	12:yWF4eguIWKvU9bEMsR5OErixCvJO1Vi5rgsM:LF4mKctEMYOK4CvJUVYM
MD5:	D6741608BA48E400A406ACA7F3464765
SHA1:	8961CA85AD82BB701436FFC64642833CFBAFF303
SHA-256:	B1DB1D8C0E5316D2C8A14E778B7220AC75ADAE5333A6D58BA7FD07F4E6EAA83C
SHA-512:	E85360DBBB0881792B86DCAF56789434152ED69E00A99202B880F19D551B8C78EEFF38A5836024F5D61DBC36818A39A921957F13FBF592BAAFD06ACB1AED244
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\pXscrbCrewUD-UetJTvW5F7YMxo.gz[1].js	
IE Cache URL:	http://https://www.bing.com/rp/pXscrbCrewUD-UetJTvW5F7YMxo.gz.js
Preview:	var BingAtWork;(function(n){var t;(function(n){function t(t,i){var u,r;t.isAuthenticated&&(n.raiseAuthEventAndLog(t),u=_ge("sb_form_q"),u&&(r=u.getAttribute("value"),r&&(n.fetchLowerHeader(r),n.fetchScopeBar(r),i.notifEnabled&&i.notifFetchAsync&&n.fetchNotificationConditional())))}function i(n,i){n&&n.length==2&&t(n[1],i)}n.bind ToConditionalSignIn=function(n){sj_evt.bind("ssofirstquery",function(t){return i(t,n)},!0,null,!1)}})(t=n.ConditionalSignIn||(n.ConditionalSignIn={}))})(BingAtWork||(Bing AtWork={}))

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\sbi[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	46137
Entropy (8bit):	5.492718429280291
Encrypted:	false
SSDEEP:	768:WkuL2ym/YIZE2u1U5l7Ez+YIdQFSO4FWCPPZPzATfZjFwummSczZxG3IuO7JUDWB:plB1FWCpPwkNijuSjyir
MD5:	8147A3C6CCDAD2147CA32BA6DB54E40A
SHA1:	3257CCC8CED1107ACBE3697B61F1C5ED3A86A4E6
SHA-256:	E783F26B771F68588FF468DE04C50E6A3E7BC4A11FEBDB52A17511E9DFE91297
SHA-512:	005695CB7F9FBB397109F11FDD375F23D5C678C7F26036E3937C916F75C96857F6A7C1B10D5820588461479A14B69026A3277389E5C02D09359D5A2BD9CF3C67
Malicious:	false
IE Cache URL:	http://https://www.bing.com/images/sbi?mmasync=1&ptn=Homepage&IID=SBI&IG=B828A7B7ED484BA496041EEF93D34E3C&form=REDIRERR
Preview:	<style type="text/css">#sbiarea,#sbicom{display:none}.hassbi #sbiarea{display:inline-block}#sbiarea{margin:0 0 0 18px}.sbox #sb_form #sbiarea{margin:0}#sb_sbi{d isplay:inline-block;cursor:pointer}img#sbi_b{vertical-align:-2px;height:20px;width:20px}#detailPage #detailheader img#sbi_b,.blue2#miniheader img#sbi_b,.sbox im g#sbi_b{vertical-align:-3px}.blue2#miniheader img#sbi_b{vertical-align:-1px}#sbi_b.grayscaled{filter:grayscale(1) brightness(1.4);-webkit-filter:grayscale(1) brightness(1 .4)}#sbi_b.grayscaled:hover{filter:grayscale(1) brightness(1);-webkit-filter:grayscale(1) brightness(1)}#sb_sbip[shdlg] #sbi_b{filter:grayscale(0);-webkit-filter:grayscal e(0)}#sb_sbip .rms_iac{display:inline-block}#sb_sbip:not(.disableTooltip):hover::before,#sb_sbip.shtip:not(.disableTooltip)::before,#sb_sbip[vptest]::before{bottom:-27px; left:10px;z-index:6}#sb_sbip:not(.disableTooltip):hover::after,#sb_sbip.shtip:not(.disableTooltip)::after,#sb_sbip[vptest]::after{top:40px;left:10px;z-index:4}#hp_contain

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\svI82uPNFRD54V4bMLaeahXQXBI.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	425
Entropy (8bit):	4.963129739598361
Encrypted:	false
SSDEEP:	12:2gXsmzwKN0yApFkRLNF1Jfa1VTWPMg9pIGywV:2gX9zwKN0yAqr1Jfa1V059V
MD5:	016ECFDB34031F881FA5E34DFBD0B7A1
SHA1:	16D3BA1049939D00AE47AAD053993B4762D9B102
SHA-256:	08021ED3BCA5532304B597E636BEB939FF7BAA6D08DCA4E94C0DDE1FDF940389
SHA-512:	D61045D1F07ED241626B8233D388F5E1AD54DBE224871E1CE872ECFD0E29F05A21F0EA02FFDE688FACB134DD969533615493BD35EBA4D5E755840C30A687EE(0
Malicious:	false
Preview:	(function(n){function f(){u(sj_be,r)}function r(i){return i&&n.enqueue(t,i),!0}function e(){u(sj_ue,r)}function u(n,t){for(var u,r=0;r<i.length;r++)u=i[r],n(u==="resize"?window:doc ument,window.navigator.pointerEnabled?u.replace("mouse","pointer"):u,t,!1)}var t="EVT",i=["click","mousedown","mouseup","touchstart","touchend","mousemove","tou chmove","scroll","keydown","resize"];n.wireup(t,{load:f,compute:null,unload:e})})(BM)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\test[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	64
Entropy (8bit):	4.373593025747649
Encrypted:	false
SSDEEP:	3:UMs1TE5LH0cHrJU4YCf:U37cVUof
MD5:	E82D9BD501B46DF5CB2B650AF9E1B126
SHA1:	0FE6876226E88D8104ED51CB6329EB172BBA8D68
SHA-256:	C2BA8FCCFC980BCC8FC24E7A41BFCFEE88CCA9331C8D4D62890D7DFAB4A12226
SHA-512:	D3715E6A3C9012F2D8E1269E5C4B3E2F77FD2CD8E793AD39E51F1E1BE30F0818DDD01FAF3708EF789FDF347B92C6477C10A1155DEC582FF68185CBFD41C662 4
Malicious:	false
Preview:	IPv6Tests.TestIPv6Response('{"type": "4"}');

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\th[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\th[1].jpg	
Size (bytes):	6795
Entropy (8bit):	7.939267233088054
Encrypted:	false
SSDEEP:	192:pPFWzMAm+TL7LZ895qWynOjJN52aPjP2D9a1R0:5FWmM7y7TZFNoaLc9Ai
MD5:	140F382635756FE19E1CD67D8CDAB923
SHA1:	1B0F1B61C068E01CE6FFDC5FFCADDD5E039D0DA5
SHA-256:	216E799943B615F3EBF0FC09391810AF53FDE0EDCBEC4300F2B01B98AF346FAE
SHA-512:	A7403C2FB1E2C858C3B3A1F6860441A8B820033E5D6E0049DF6922A1BFB0F74180A2538CFD82F292219629FB1FCA6AB8D3AAAA97129C4C86BC8D15FACDD405F3
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fk3tJ.img&ehk=VNetxfVLBzRQk0Hk9PeD6wuxhnc6QG%2bQVORzTT762Ms%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....,.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====..."....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...3Fj.E.[.$\..M..+.ij.!...{..,.....j\..|.\....>..7.....}kVo.(bD..U...Pj....XO.....$.[..|....<...p._0..n*...k..O...D6.L.`....?..U-..D...f.....h.'z^(...&j...[h:S..."....O.k.o...7..@..`.n.~R.....Px...m ;.3X...E.....D..Cm.$..8>....F(...VrB.1..4S.....u.&.w.Oe3...1.C..2.....1..5.j.....!&._..n.h...'.r.=I..y...Y..2.\....a$...$.;.$..v.,.....YR..%.....;.N

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\th[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	4579
Entropy (8bit):	7.899738415633208
Encrypted:	false
SSDEEP:	96:pPElQIszgVi+8yJg1On37lfYKgsaU4AzO/wVie:pPk50gd8ysW5QKgizce
MD5:	6252E142AFB55FA1C5DD093059E5B784
SHA1:	FA2DEDFB97B7BF7B2D1052EA4B0DEC214E4217A1
SHA-256:	24461B5094C1DC8AA9F6741AD78006FF35954478933E003E2CD036EA8E303EA4
SHA-512:	A6156F1C962CE251B79C86F5A5B5BBA8C3D8C1060251CD69365C650D5BF2480ED14A6F36CFF4235BB0E53DC15903086CF901891B2DEEC050271A851D88C3DE
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fket7.img&ehk=x1iCxRdz8nKwKjWtFCBaxEx1tovE7Q0NcYc3bmTeH%2fl%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....,.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====..."....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..f..$H.."(.f'..rk..9.....B<...9.c.:...E,.....=...w....._h.....yttW=.....tr..>l0..+.fE..,z..s..js.....5,.....i.....+.Cm=.3Sj.6.|.r...>.G.....W.Z.]){..i[..&.C...,.*A...s.u.....s.S.>ni..t.;....OH..i.3N.R.[..2..7..*.#.}SP..O.X@.....zt98.YzR..2..9.`Y..r..ZN.,..+9Tp.....C.cS.>.PT..X.....S..8S..moJV..<.>..Z.U.).7ZV..!..h.0.S.\..eX5k)..Gp.O....J..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\6sxhavkE4_SZHA_K4rwWmg67vF0.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	20320
Entropy (8bit):	5.35616705330287
Encrypted:	false
SSDEEP:	384:Kh4xTJXiXZ4sb4ZENXjTDDoFWZ3BnqIfP5IDV6s4RKAvKXAL5Nuwbv++9O:YoTdiJpjBpBnqIH+Z6se4XALueO
MD5:	07F6B49331D0BD13597934A20FAC385B
SHA1:	B39E1439D7FC072AF4961D4AB6DE07D0BC64B986
SHA-256:	4752E030AC235C73E92EC8BBF124D9A32A424457CA9A6D6027A9595DA76F98D7
SHA-512:	333B12B6BC7F72156026829E820A4F24759E15973B474E2FFB264DEE4C50B0E478128255E416F3194E8C170A28DF02AA425D720CC5E15BC2382EA2D6D57A6F5B
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/6sxhavkE4_SZHA_K4rwWmg67vF0.gz.js
Preview:	/*!DisableJavascriptProfiler*/.var BM=BM||{};BM.config={B:{timeout:250,delay:750,maxUrlLength:300,sendlimit:20,maxPayloadSize:14e3},V:{distance:20},N:{maxUrlLength:300},E:{buffer:30,timeout:5e3,maxUrlLength:300},C:{distance:10}},function(n){function vt(){if(!document.querySelector||!document.querySelectorAll){k({FN:"init",S:"QuerySelector"});return}w={};e=[];ft=1;ut=0;rt=0;o=[];s=0;h=!1;var n=Math.floor(Math.random()*1e4).toString(36);t={P:{C:0,N:0,I:n,S:fi,M:r,T:0,K:r,F:0}};vi()}function ei(n,t){var r={};for(var i in n)i.indexOf("_")!==0&&(i in t&&(n[i]!==t[i]||i==="i")?(r[i]=t[i],n[i]=t[i]):r[i]=null);return r}function oi(n){var i={};for(var t in n)n.hasOwnProperty(t)&&(i[t]=n[t]);return i}function b(n,t,r,u){if(!h){k({FN:"snapshot",S:n});return}r=r||gt;t=t||!1;var f=g()+r;ot(o,n)===-1&&o.push(n);t?(yt(),pt(t,u)):f>s&&(yt(),rt=sb_st(pt,r),s=f)}function k(n){var u={T:"CI.BoxModelError",FID:"CI",Name:ht,SV:ct,P:t&&"P"in t?d(t.P):r,TS:f(),ST:v},i,e;for(i in n)u[i]=n[i];e=d(u);wt(e)}func

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\BJp5dDFvoQm12CHBfp4PC6aiyg4.gz[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):	73202

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\BJp5dDFvoQm12CHBfp4PC6aiyg4.gz[1].css	
Entropy (8bit):	5.307816444057117
Encrypted:	false
SSDEEP:	1536:kcGJTL/mKzAAFl7JlsG0GRe1cxnoWC1kuyOYkTs/Kun:LGJ4AFl7JlsG0GRCcxnoWC1kuyOYkT0
MD5:	C912DA2683E71660357A600EE34A7873
SHA1:	5DFD028307D4CD8A66492E807B848FEC177AEC3A
SHA-256:	525D57B5D38D8212993C66A33F4CD15EDBD0F260A5AFCF539D092047A908D6EE
SHA-512:	31E2A56C27CC037AD903292DFA518E86642C2A610E9923DD4F7A2FD1347167E042E957A85E98561CC9178318D121DEA3EF165F88EEC79915D0687939DC25BBC
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/BJp5dDFvoQm12CHBfp4PC6aiyg4.gz.css
Preview:	.scopes{color:rgba(255,255,255,.8);display:inline-block;left:0;white-space:nowrap;list-style:none;line-height:39px}.scopes.sc_hide{display:none}.scopes .scope{font-size:.8125rem;cursor:pointer;vertical-align:middle;margin-right:36px;background-repeat:no-repeat;position:relative;display:inline-block}.scopes .scope:hover,.scopes .scope.focusin{color:#fff}.scopes .scope:hover .overflow_menu,.scopes .scope.focusin .overflow_menu{transform:none}.scopes .scope:focus-within .overflow_menu{color:#fff;transform:none}.scopes .scope a{color:inherit;cursor:pointer;text-decoration:none}.scopes .scope.dots{margin-bottom:8px;font-weight:bold}.scopes .scope.dots:before{display:inline-block;content:'. . .'}.scopes .scope.dots.hover_focus:focus{outline:none}.scopes .scope .overflow_menu{color:#666;cursor:pointer;transform:scale(0);position:absolute;background-color:#fff;border-radius:6px;padding:4px 0;box-shadow:0 4px 12px 1px rgba(0,0,0,.14);min-width:155px}.scopes .scope .overflow_menu .overflow_item{

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\JDHEvZVDnqsG9UcxzgIdtGb6thw.gz[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):	408
Entropy (8bit):	5.040387533075148
Encrypted:	false
SSDEEP:	12:2QWV6yRZ1nkDXAn357CXYX0cO2mAICL2b3TRn:2QO6P+5OYXJPi3TRn
MD5:	B4D53E840DB74C55CC3E3E6B44C3DAC1
SHA1:	89616D8595CF2D26B581287239AFB62655426315
SHA-256:	622B88D7D03DDACC92B81FE80A30B3D5A04072268BF9473BB29621E884AAB5F6
SHA-512:	4798E4E1E907EAE161E67B9BAB42206CE0F22530871EEC63582161E29DD00D2D7034E7D12CB3FE56FFF673BC9BB01F0646F9CA5DAED288134CB25978EFBBECF
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/JDHEvZVDnqsG9UcxzgIdtGb6thw.gz.js
Preview:	(function(){function u(){n&&(n.value.length>0?Lib.CssClass.add(sj_b,t):Lib.CssClass.remove(sj_b,t))}function f(r){n.value="";Lib.CssClass.remove(sj_b,t);sj_log("CI.XButton","Clicked","1");i&&Lib.CssClass.add(i,"b_focus");n.focus();n.click();r&&(r.preventDefault(),r.stopPropagation())}var i=_ge("b_header"),n=_ge("sb_form_q"),r=_ge("sb_clt"),t="b_sbText";n&&r&&(sj_be(r,"click",f),sj_be(n,"keyup",u),u())})()

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\NnFHhz2jL6yzChtIhaB5IIVKY5k[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1111
Entropy (8bit):	4.61511796141903
Encrypted:	false
SSDEEP:	24:twgonGLheJUVYxCdBTMqTS05sLGkkhQgbQgwHW4QhJ:6gAShpyxCdBTrS05sLKhvUfSJ
MD5:	C04C8834AC91802186E6CE677AE4A89D
SHA1:	367147873DA32FACB30A1B4885A07920854A6399
SHA-256:	46CC84BA382B065045DB005E895414686F2E76B64AF854F5AD1AC0DF020C3BDB
SHA-512:	82388309085BD143E32981FE4C79604DCEFC4222FB2B53A8625852C3572BDE3D3A578DD558478E6A18F7863CC4EC19DFBA3EE78AD8A4CC71917BFFE027DC220
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/NnFHhz2jL6yzChtIhaB5IIVKY5k.svg
Preview:	<svg width="20px" height="16px" viewBox="0 0 20 16" focusable="false" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">.. <g transform="translate(-10, -12)" fill="#007DAA" >.. <path d="M28.125,14.4615385 L25,14.4615385 L24.26875,13.0203077 C23.95125,12.3950769 23.30125,12 22.59125,12 L17.40875,12 C16.69875,12 16.04875,12.3950769 15.73125,13.0203077 L15,14.4615385 L11.875,14.4615385 C10.84,14.4615385 10,15.2886154 10,16.3076923 L10,26.1538462 C10,27.1729231 10.84,28 11.875,28 L28.125,28 C29.16,28 30,27.1729231 30,26.1538462 L30,16.3076923 C30,15.2886154 29.16,14.4615385 28.125,14.4615385 Z M20,25.5384615 C17.23875,25.5384615 15,23.3341538 15,20.6153846 C15,17.8966154 17.23875,15.6923077 20,15.6923077 C22.76125,15.6923077 25,17.8966154 25,20.6153846 C25,23.3341538 22.76125,25.5384615 20,25.5384615 Z M20,18.1538462 C18.62125,18.1538462 17.5,19.2578462 17.5,20.6153846 C17.5,21.9729231 18.62125,23.0769231 20,23.0769231 C21.37875,23.0769231

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\P3LN8DHh0udC9Pbh8UHnw5FJ8R8.gz[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):	1516
Entropy (8bit):	5.30762660027466
Encrypted:	false
SSDEEP:	24:+FE64YTsQF61KWlWeM2lSoiLKiUfpIYdk+fzvOMuHMH34tDO8XgGQE3BUf4JPwk:+FdF6UYXEBi9kIHIB1UY

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\P3LN8DHh0udC9Pbh8UHnw5FJ8R8.gz[1].js	
MD5:	EF3DA257078C6DD8C4825032B4375869
SHA1:	35FE0961C2CAF7666A38F2D1DE2B4B5EC75310A1
SHA-256:	D94AC1E4ADA7A269E194A8F8F275C18A5331FE39C2857DCED3830872FFAE7B15
SHA-512:	DBA7D04CDF199E68F04C2FECFDADE32C2E9EC20B4596097285188D96C0E87F40E3875F65F6B1FF5B567DCB7A27C3E9E8288A97EC881E00608E8C6798B24EF3F
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/P3LN8DHh0udC9Pbh8UHnw5FJ8R8.gz.js
Preview:	var Identity=Identity||{},ham_id_js_downloaded=!1;(function(n,t,i,r,u,f,e){e.wlProfile=function(){var r=sj_cook.get,u="WLS",t=r(u,"N"),i=r(u,"C");return i&&e.wlImgSm&&e.wlImgLg?{displayName:t?t.replace(/\+/g," "):"",name:n(t.replace(/\+/g," ")),img:e.wlImgSm.replace(/\{0\}/g,f(i)),imgL:e.wlImgLg.replace(/\{0\}/g,f(i)),idp:"WL"}:null};e.headerLoginMode=0;e.popupAuthenticate=function(n,i,r){var o,u,h,c,v=sb_gt(),l=Math.floor(v/1e3).toString(),s="ct",a=new RegExp("([?&])"+s+"=.*?(&|$)","i");return n.toString()==="WindowsLiveId"&&(o=e.popupLoginUrls,u=o[n],u=u.match(a)?u.replace(a,"$1"+s+"="+l+"$2"):u+"?"+s+"="+l,e.popupLoginUrls.WindowsLiveId=u),(o=e.popupLoginUrls)&&(u=o[n]+(i?"&perms="+f(i):"")+(r?"&src="+f(r):""))&&(h=e.pop(u))&&(c=setInterval(function(){h.closed&&(t.fire("id:popup:close"),clearInterval(c))},100))};e.pop=function(n){return r.open(n,"idl","location=no,menubar=no,resizable=no,scrollbars=yes,status=no,titlebar=no,toolbar=no,width=1000,height=620")};var o=u("id_h"),s=u("id

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\Passport[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	329
Entropy (8bit):	5.086971439676268
Encrypted:	false
SSDEEP:	6:qzxUe3X965+zAqEFtTNfYEAn4TXQ3SOFCL0H4WZhCroOI:kxFkXq6tTRYEVTAx4IHH7CroOI
MD5:	7B7D5DA1B057EB0D5A58C2585E80BACA
SHA1:	29714CD8C570E321C1C1C991E77ACE3945312AC6
SHA-256:	023CD9B7315636BE1BE24DC78144554B0E76777BD476ED581378172DE9B12A05
SHA-512:	1A4E36E3124968166579C04D05A1325242E1DFE20DF4C804081487A019B88395A679A439525488F78B73334C5B0BD38D61E24F8E23F2F8274C6BAC323291CEE8
Malicious:	false
IE Cache URL:	http://https://www.bing.com/secure/Passport.aspx?popup=1&ssl=1
Preview:	<html><head><title>Bing</title></head><body>Loading...<script type="application/x-javascript">//<![CDATA[.var _w = window; var o = _w.opener; var mainWindow; (mainWindow = o) || (mainWindow = _w.parent); if (mainWindow) {mainWindow.sj_evt && mainWindow.sj_evt.fire("wl:cancel"); };if (o) _w.close();;.// </script></body></html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8_2B[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gzip compressed data, max speed, from TOPS/20
Category:	dropped
Size (bytes):	369
Entropy (8bit):	7.381606070228713
Encrypted:	false
SSDEEP:	6:XtA9/UWowHIYpLf27o3Q8QXoxRgqIDk+f0j7Bso3nka0LUpaflSIwo:XwUWesAZXoozD/f9SkaVpho
MD5:	9EC7CD87F69909EF5BEC476FB8988714
SHA1:	13CBDAA33357C7422C29C8E148DC1DEEFF2DA5EE
SHA-256:	5216370944CA0A0FFB66437DB68CEE5DA1E4926CE295054FE7C48272477E0662
SHA-512:	3F77206C22DECDB3ECDF0D05342BA1DA411D73AE5658BF24AB77C3515C67C2D922E1F463F0D439A7F9850332742E287E8FA5EB4D055129929C7B186C6F5ECDD1
Malicious:	false
Preview:	.....T.Os.0.@..wpz.?...6.#.n....''...0."...;.....J.f.%.....g..^.Z.P.f.....y|...O.i....BN.2.....1...K.U.....JU%.0X..w...j.Q..-#.....!..G..].....y.....U...s..ipB..>R..f.G.....`^[d.~u.a....<.m..6..p.V....#.\L....fx....Y...../.s...7.^|[..M$.h.n.....'o7...N.!.'..YQ...`.....H.t.g.dH..`.Fcol.....L..s..2./-|5..5.../.....Gb.>....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\bLULVERLX4vU6bjspboNMw9vl_0.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	very short file (no magic)
Category:	downloaded
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A99
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/bLULVERLX4vU6bjspboNMw9vl_0.gz.js
Preview:	0

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.609910778918113
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	0204.gif.dll
File size:	112796
MD5:	75c8d835dbb17059c37f5bbe70736e4e
SHA1:	12f7c7f15b85ef34ba3f77a364dcc480c99b6eda
SHA256:	8b130f9fbdcfc64e2ef698a1f111409c66aff2ab6ce66ae0286f8c6817376064
SHA512:	5afccf505dad49a9ecd3b3c9a9a95e831ed4a1e58e42ab157b21fd495c99e8434207a2edd4e5552307360cee051e8557a0449fe053c35569e47f02df7d5bad5c
SSDEEP:	1536:DWKaY5Se9WnVI78XvnoxJasJvRHKmyGDvDk0Rt9Y56l5ZMpvV05o9OX5xPw8:DWa0eQnVI7qCqZGDvDk4wol5w0EU
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._W...6e..6e..6e..)v..6e...w..6e.Rich.6e.....PE..L.....f`.....!.....Z.....`.....p.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10006099
Entrypoint Section:	.code
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x6066E9D0 [Fri Apr 2 09:54:24 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	811de8e945c2087a6e052096546cd842

Entrypoint Preview

Instruction
push ebx
push ebx
and dword ptr [esp], 00000000h
add dword ptr [esp], ebp
mov ebp, esp
add esp, FFFFFFF8h

Instruction
push esi
mov dword ptr [esp], FFFF0000h
call 00007F840093A5C0h
push ecx
add dword ptr [esp], 00000247h
sub dword ptr [esp], ecx
push ecx
mov dword ptr [esp], 00005267h
call 00007F8400936F69h
push esi
mov esi, eax
or esi, eax
mov eax, esi
pop esi
jne 00007F840093C062h
pushad
push 00000000h
mov dword ptr [esp], edi
xor edi, edi
or edi, dword ptr [ebx+0041856Bh]
mov eax, edi
pop edi
push edx
add dword ptr [esp], 40h
sub dword ptr [esp], edx
push ebx
mov dword ptr [esp], 00001000h
push edi
sub dword ptr [esp], edi
xor dword ptr [esp], eax
push 00000000h
call dword ptr [ebx+0045D014h]
mov dword ptr [ebp-04h], ecx
and ecx, 00000000h
xor ecx, eax
and edi, 00000000h
or edi, ecx
mov ecx, dword ptr [ebp-04h]
push eax
sub eax, dword ptr [esp]
or eax, edi
and dword ptr [ebx+0041809Bh], 00000000h
xor dword ptr [ebx+0041809Bh], eax
pop eax
cmp ebx, 00000000h
jbe 00007F840093C03Eh
add dword ptr [ebx+004180F7h], ebx
add dword ptr [ebx+00418633h], ebx
mov dword ptr [ebp-04h], edx
sub edx, edx
xor edx, dword ptr [ebx+004180F7h]
mov esi, edx
mov edx, dword ptr [ebp-04h]
push edi
xor edi, dword ptr [esp]
xor edi, dword ptr [ebx+0041856Bh]
and ecx, 00000000h
or ecx, edi
pop edi
cld
rep movsb
push ebx
mov dword ptr [eax+eax], 00000000h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x17000	0x51	.data
IMAGE_DIRECTORY_ENTRY_IMPORT	0x5d050	0x64	.data
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x5d000	0x50	.data
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.code	0x1000	0x15966	0x15a00	False	0.70799087789	data	6.48337924377	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x17000	0x51	0x200	False	0.140625	data	0.863325225156	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rdata	0x18000	0x44c5f	0x1800	False	0.13330078125	data	0.926783139034	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.data	0x5d000	0x250	0x400	False	0.2900390625	data	2.96075631554	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
user32.dll	GetActiveWindow, CheckDlgButton, CheckMenuItem, CheckRadioButton, CheckMenuRadioItem
kernel32.dll	GetProcAddress, LoadLibraryA, VirtualProtect, VirtualAlloc, lstrlenA, GetCurrentThreadId, GetCurrentProcess, GetCurrentThread, Module32FirstW
ole32.dll	OleInitialize
comctl32.dll	DPA_Sort

Exports

Name	Ordinal	Address
StartService	1	0x1000b959

Network Behavior

Network Port Distribution

Total Packets: 89

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 09:56:46.039710999 CEST	49742	80	192.168.2.5	185.243.114.196
Apr 6, 2021 09:56:46.039738894 CEST	49741	80	192.168.2.5	185.243.114.196
Apr 6, 2021 09:56:47.050151110 CEST	49741	80	192.168.2.5	185.243.114.196
Apr 6, 2021 09:56:47.051136971 CEST	49742	80	192.168.2.5	185.243.114.196
Apr 6, 2021 09:56:47.208869934 CEST	49743	80	192.168.2.5	185.243.114.196
Apr 6, 2021 09:56:47.209781885 CEST	49744	80	192.168.2.5	185.243.114.196
Apr 6, 2021 09:56:48.223792076 CEST	49743	80	192.168.2.5	185.243.114.196
Apr 6, 2021 09:56:48.378180981 CEST	49744	80	192.168.2.5	185.243.114.196
Apr 6, 2021 09:56:49.065798998 CEST	49741	80	192.168.2.5	185.243.114.196
Apr 6, 2021 09:56:49.066380024 CEST	49742	80	192.168.2.5	185.243.114.196
Apr 6, 2021 09:56:50.237746000 CEST	49743	80	192.168.2.5	185.243.114.196
Apr 6, 2021 09:56:50.378489017 CEST	49744	80	192.168.2.5	185.243.114.196
Apr 6, 2021 09:56:53.094451904 CEST	49746	80	192.168.2.5	185.243.114.196
Apr 6, 2021 09:56:53.094507933 CEST	49747	80	192.168.2.5	185.243.114.196
Apr 6, 2021 09:56:54.081844091 CEST	49746	80	192.168.2.5	185.243.114.196
Apr 6, 2021 09:56:54.082014084 CEST	49747	80	192.168.2.5	185.243.114.196
Apr 6, 2021 09:56:54.402477026 CEST	49748	80	192.168.2.5	185.243.114.196
Apr 6, 2021 09:56:55.394422054 CEST	49748	80	192.168.2.5	185.243.114.196
Apr 6, 2021 09:56:56.081964970 CEST	49746	80	192.168.2.5	185.243.114.196
Apr 6, 2021 09:56:56.082747936 CEST	49747	80	192.168.2.5	185.243.114.196
Apr 6, 2021 09:56:57.410167933 CEST	49748	80	192.168.2.5	185.243.114.196
Apr 6, 2021 09:57:23.127945900 CEST	49752	80	192.168.2.5	185.186.244.95
Apr 6, 2021 09:57:23.128319025 CEST	49751	80	192.168.2.5	185.186.244.95
Apr 6, 2021 09:57:24.131153107 CEST	49751	80	192.168.2.5	185.186.244.95
Apr 6, 2021 09:57:24.131201029 CEST	49752	80	192.168.2.5	185.186.244.95
Apr 6, 2021 09:57:24.355110884 CEST	49753	80	192.168.2.5	185.186.244.95
Apr 6, 2021 09:57:24.356322050 CEST	49754	80	192.168.2.5	185.186.244.95
Apr 6, 2021 09:57:25.365633965 CEST	49753	80	192.168.2.5	185.186.244.95
Apr 6, 2021 09:57:25.367499113 CEST	49754	80	192.168.2.5	185.186.244.95
Apr 6, 2021 09:57:26.147221088 CEST	49751	80	192.168.2.5	185.186.244.95
Apr 6, 2021 09:57:26.147244930 CEST	49752	80	192.168.2.5	185.186.244.95
Apr 6, 2021 09:57:27.366352081 CEST	49753	80	192.168.2.5	185.186.244.95
Apr 6, 2021 09:57:27.366364002 CEST	49754	80	192.168.2.5	185.186.244.95
Apr 6, 2021 09:57:30.163558006 CEST	49755	80	192.168.2.5	185.186.244.95
Apr 6, 2021 09:57:30.163878918 CEST	49756	80	192.168.2.5	185.186.244.95
Apr 6, 2021 09:57:31.178636074 CEST	49755	80	192.168.2.5	185.186.244.95
Apr 6, 2021 09:57:31.180039883 CEST	49756	80	192.168.2.5	185.186.244.95
Apr 6, 2021 09:57:31.382344007 CEST	49757	80	192.168.2.5	185.186.244.95
Apr 6, 2021 09:57:32.381802082 CEST	49757	80	192.168.2.5	185.186.244.95
Apr 6, 2021 09:57:33.178752899 CEST	49755	80	192.168.2.5	185.186.244.95
Apr 6, 2021 09:57:33.178978920 CEST	49756	80	192.168.2.5	185.186.244.95

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 09:55:12.321458101 CEST	52212	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:55:12.332722902 CEST	53	52704	8.8.8.8	192.168.2.5
Apr 6, 2021 09:55:12.367438078 CEST	53	52212	8.8.8.8	192.168.2.5
Apr 6, 2021 09:55:12.444320917 CEST	54302	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:55:12.490284920 CEST	53	54302	8.8.8.8	192.168.2.5
Apr 6, 2021 09:55:12.825433969 CEST	53784	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:55:12.881592989 CEST	53	53784	8.8.8.8	192.168.2.5
Apr 6, 2021 09:55:15.647516012 CEST	65307	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:55:15.701771021 CEST	53	65307	8.8.8.8	192.168.2.5
Apr 6, 2021 09:55:39.234160900 CEST	64344	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:55:39.293535948 CEST	53	64344	8.8.8.8	192.168.2.5
Apr 6, 2021 09:55:39.665812969 CEST	62060	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:55:39.716193914 CEST	53	62060	8.8.8.8	192.168.2.5
Apr 6, 2021 09:55:41.708216906 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:55:41.754092932 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 6, 2021 09:55:42.584359884 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:55:42.633232117 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 6, 2021 09:55:49.585715055 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:55:49.634418011 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 6, 2021 09:55:51.808877945 CEST	61733	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:55:51.854863882 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 6, 2021 09:55:52.675323009 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:55:52.721487045 CEST	53	65447	8.8.8.8	192.168.2.5
Apr 6, 2021 09:55:53.527688026 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:55:53.573759079 CEST	53	52441	8.8.8.8	192.168.2.5
Apr 6, 2021 09:55:57.473318100 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:55:57.531478882 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 6, 2021 09:55:58.623642921 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:55:58.672686100 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 6, 2021 09:55:59.530352116 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:55:59.577027082 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 6, 2021 09:55:59.891972065 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:55:59.962860107 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:00.110093117 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:56:00.157924891 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:00.813059092 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:56:00.861538887 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:01.153757095 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:56:01.200303078 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:56:01.206017017 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:01.258028030 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:01.302402020 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:56:01.373768091 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:01.824034929 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:56:01.869940996 CEST	53	60075	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:01.899358988 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:56:01.946440935 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:56:01.946448088 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:01.995270014 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:02.913166046 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:56:02.958863974 CEST	53	57128	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:03.081171036 CEST	54791	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:56:03.129930019 CEST	53	54791	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:06.190893888 CEST	50463	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:56:06.245198011 CEST	53	50463	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:06.705409050 CEST	50394	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:56:06.759615898 CEST	53	50394	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:07.973144054 CEST	58530	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:56:08.045044899 CEST	53813	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:56:08.056432962 CEST	53	58530	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:08.099992037 CEST	53	53813	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:26.152525902 CEST	63732	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:56:26.199120998 CEST	53	63732	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:27.142621994 CEST	63732	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 09:56:27.189728022 CEST	53	63732	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:27.371381998 CEST	57344	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:56:27.422842026 CEST	53	57344	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:28.158164024 CEST	63732	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:56:28.204546928 CEST	53	63732	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:30.175906897 CEST	63732	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:56:30.221748114 CEST	53	63732	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:32.070358992 CEST	54450	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:56:32.129595041 CEST	53	54450	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:34.190895081 CEST	63732	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:56:34.236850023 CEST	53	63732	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:44.671691895 CEST	59261	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:56:44.727936983 CEST	53	59261	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:45.961915970 CEST	57151	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:56:46.016486883 CEST	53	57151	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:47.151609898 CEST	59413	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:56:47.200351954 CEST	53	59413	8.8.8.8	192.168.2.5
Apr 6, 2021 09:56:52.340157032 CEST	60516	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:56:52.405512094 CEST	53	60516	8.8.8.8	192.168.2.5
Apr 6, 2021 09:57:00.114474058 CEST	51649	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:57:00.168636084 CEST	53	51649	8.8.8.8	192.168.2.5
Apr 6, 2021 09:57:01.418694019 CEST	65086	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:57:01.472898960 CEST	53	65086	8.8.8.8	192.168.2.5
Apr 6, 2021 09:57:03.284967899 CEST	56432	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:57:03.331330061 CEST	53	56432	8.8.8.8	192.168.2.5
Apr 6, 2021 09:57:05.699322939 CEST	52929	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:57:05.759550095 CEST	53	52929	8.8.8.8	192.168.2.5
Apr 6, 2021 09:57:21.815330029 CEST	64317	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:57:21.875345945 CEST	53	64317	8.8.8.8	192.168.2.5
Apr 6, 2021 09:57:23.050957918 CEST	61004	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:57:23.108716011 CEST	53	61004	8.8.8.8	192.168.2.5
Apr 6, 2021 09:57:24.288322926 CEST	56895	53	192.168.2.5	8.8.8.8
Apr 6, 2021 09:57:24.344851971 CEST	53	56895	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 6, 2021 09:56:01.200303078 CEST	192.168.2.5	8.8.8.8	0x52c9	Standard query (0)	login.micr osoftonline.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:56:01.899358988 CEST	192.168.2.5	8.8.8.8	0x662e	Standard query (0)	login.micr osoftonline.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:56:45.961915970 CEST	192.168.2.5	8.8.8.8	0x3557	Standard query (0)	under17.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:56:47.151609898 CEST	192.168.2.5	8.8.8.8	0x23a6	Standard query (0)	under17.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:57:00.114474058 CEST	192.168.2.5	8.8.8.8	0xedfc	Standard query (0)	under17.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:57:01.418694019 CEST	192.168.2.5	8.8.8.8	0x39b2	Standard query (0)	under17.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:57:23.050957918 CEST	192.168.2.5	8.8.8.8	0x6d1	Standard query (0)	urs-world.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:57:24.288322926 CEST	192.168.2.5	8.8.8.8	0x8e59	Standard query (0)	urs-world.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 6, 2021 09:56:01.258028030 CEST	8.8.8.8	192.168.2.5	0x52c9	No error (0)	login.micr osoftonline.com	a.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 09:56:01.258028030 CEST	8.8.8.8	192.168.2.5	0x52c9	No error (0)	a.privatel ink.msiden tity.com	prda.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 09:56:01.258028030 CEST	8.8.8.8	192.168.2.5	0x52c9	No error (0)	prda.aadg. msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 6, 2021 09:56:01.373768091 CEST	8.8.8.8	192.168.2.5	0x5c4	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 09:56:01.946448088 CEST	8.8.8.8	192.168.2.5	0x662e	No error (0)	login.microsoftonline.com	a.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 09:56:01.946448088 CEST	8.8.8.8	192.168.2.5	0x662e	No error (0)	a.privatelink.msidentity.com	prda.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 09:56:01.946448088 CEST	8.8.8.8	192.168.2.5	0x662e	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 09:56:01.995270014 CEST	8.8.8.8	192.168.2.5	0xfa81	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 09:56:46.016486883 CEST	8.8.8.8	192.168.2.5	0x3557	No error (0)	under17.com		185.243.114.196	A (IP address)	IN (0x0001)
Apr 6, 2021 09:56:47.200351954 CEST	8.8.8.8	192.168.2.5	0x23a6	No error (0)	under17.com		185.243.114.196	A (IP address)	IN (0x0001)
Apr 6, 2021 09:57:00.168636084 CEST	8.8.8.8	192.168.2.5	0xedfc	No error (0)	under17.com		185.243.114.196	A (IP address)	IN (0x0001)
Apr 6, 2021 09:57:01.472898960 CEST	8.8.8.8	192.168.2.5	0x39b2	No error (0)	under17.com		185.243.114.196	A (IP address)	IN (0x0001)
Apr 6, 2021 09:57:23.108716011 CEST	8.8.8.8	192.168.2.5	0x6d1	No error (0)	urs-world.com		185.186.244.95	A (IP address)	IN (0x0001)
Apr 6, 2021 09:57:24.344851971 CEST	8.8.8.8	192.168.2.5	0x8e59	No error (0)	urs-world.com		185.186.244.95	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: loaddll32.exe PID: 6356 Parent PID: 5588

General

Start time:	09:55:20
Start date:	06/04/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\0204.gif.dll'
Imagebase:	0x10d0000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.442401635.0000000003B4D000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.362707401.0000000003C4B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.362777814.0000000003C4B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.498490060.0000000001580000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.362687587.0000000003C4B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.499756612.0000000003A4F000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.362750136.0000000003C4B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.362737439.0000000003C4B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.362723633.0000000003C4B000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6364 Parent PID: 6356

General

Start time:	09:55:20
Start date:	06/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\0204.gif.dll',#1
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6376 Parent PID: 6356

General

Start time:	09:55:21
Start date:	06/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\0204.gif.dll,StartService
Imagebase:	0x2c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.260461688.0000000002BE0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6388 Parent PID: 6364

General

Start time:	09:55:21
Start date:	06/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\0204.gif.dll',#1
Imagebase:	0x2c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.500504435.000000000562F000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.363000651.000000000582B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.499116859.0000000003490000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.445053203.000000000572D000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.363042900.000000000582B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.363073558.000000000582B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.362981300.000000000582B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.363016213.000000000582B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.363030214.000000000582B000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 5920 Parent PID: 792

General

Start time:	09:55:54
Start date:	06/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff674450000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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

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

Analysis Process: iexplore.exe PID: 6660 Parent PID: 5920

General

Start time:	09:55:57
Start date:	06/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5920 CREDAT:17410 /prefetch:2
Imagebase:	0x10d0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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

Analysis Process: iexplore.exe PID: 3440 Parent PID: 5920

General

Start time:	09:55:58
Start date:	06/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5920 CREDAT:17414 /prefetch:2
Imagebase:	0x10d0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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

Analysis Process: iexplore.exe PID: 5184 Parent PID: 792

General

Start time:	09:56:43
Start date:	06/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff674450000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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

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

Analysis Process: iexplore.exe PID: 5216 Parent PID: 5184

General

Start time:	09:56:44
Start date:	06/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5184 CREDAT:17410 /prefetch:2
Imagebase:	0xc0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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

Analysis Process: iexplore.exe PID: 3440 Parent PID: 5184

General

Start time:	09:56:45
Start date:	06/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5184 CREDAT:82948 /prefetch:2
Imagebase:	0xc0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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

Analysis Process: iexplore.exe PID: 5340 Parent PID: 792

General

Start time:	09:57:20
Start date:	06/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff674450000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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

Analysis Process: iexplore.exe PID: 3228 Parent PID: 5340

General

Start time:	09:57:21
Start date:	06/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5340 CREDAT:17410 /prefetch:2
Imagebase:	0xc0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 3708 Parent PID: 5340

General

Start time:	09:57:22
Start date:	06/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5340 CREDAT:17414 /prefetch:2
Imagebase:	0xc0000

File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis