ID: 382183
Sample Name: KcFVz0y2si.dll
Cookbook: default.jbs
Time: 22:35:48
Date: 05/04/2021
Version: 31.0.0 Emerald

Table of Contents

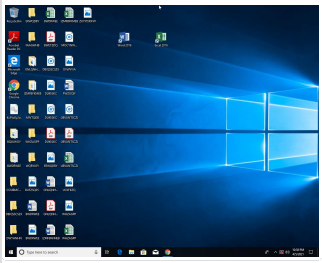
Analysis Report KcFVz0y2si.dll

Overview

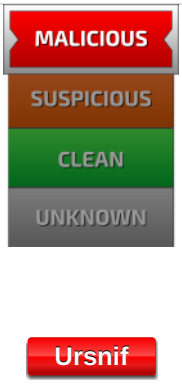
General Information

Sample Name:	KcFVz0y2si.dll
Analysis ID:	382183
MD5:	a1e2a075992485..
SHA1:	7ebf1673c6661cf..
SHA256:	657455d2129ca0..
Tags:	dll Gozi ISFB Ursnif
Infos:	

Most interesting Screenshot:



Detection



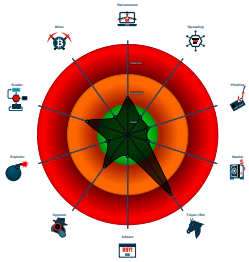
Ursnif

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: 4200 cmdline: loaddll32.exe 'C:\Users\user\Desktop\KcFVz0y2si.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 2936 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\KcFVz0y2si.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 408 cmdline: rundll32.exe 'C:\Users\user\Desktop\KcFVz0y2si.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1852 cmdline: rundll32.exe C:\Users\user\Desktop\KcFVz0y2si.dll,StartService MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 5740 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1260 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5740 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 2212 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4592 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2212 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5348 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2212 CREDAT:17414 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 1076 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 2440 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1076 CREDAT:17410 /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": "103010293JSJUYDWG",
    "sleep_time": "10",
    "SetWaitableTimer_value": "0",
    "DGA_count": "10"
  }
]
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000003.800812479.0000000004D38000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.800782996.0000000004D38000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.798289692.0000000003ACB000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.800751690.0000000004D38000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.798356915.0000000003ACB000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 15 entries				

Unpacked PEs

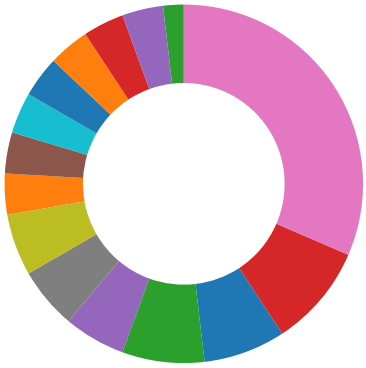
Source	Rule	Description	Author	Strings
3.2.rundll32.exe.10000000.5.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.2.rundll32.exe.1d0000.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.loaddll32.exe.1180000.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.2.rundll32.exe.11d0000.1.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	

Sigma Overview

No Sigma rule has matched

Signature Overview

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



- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

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

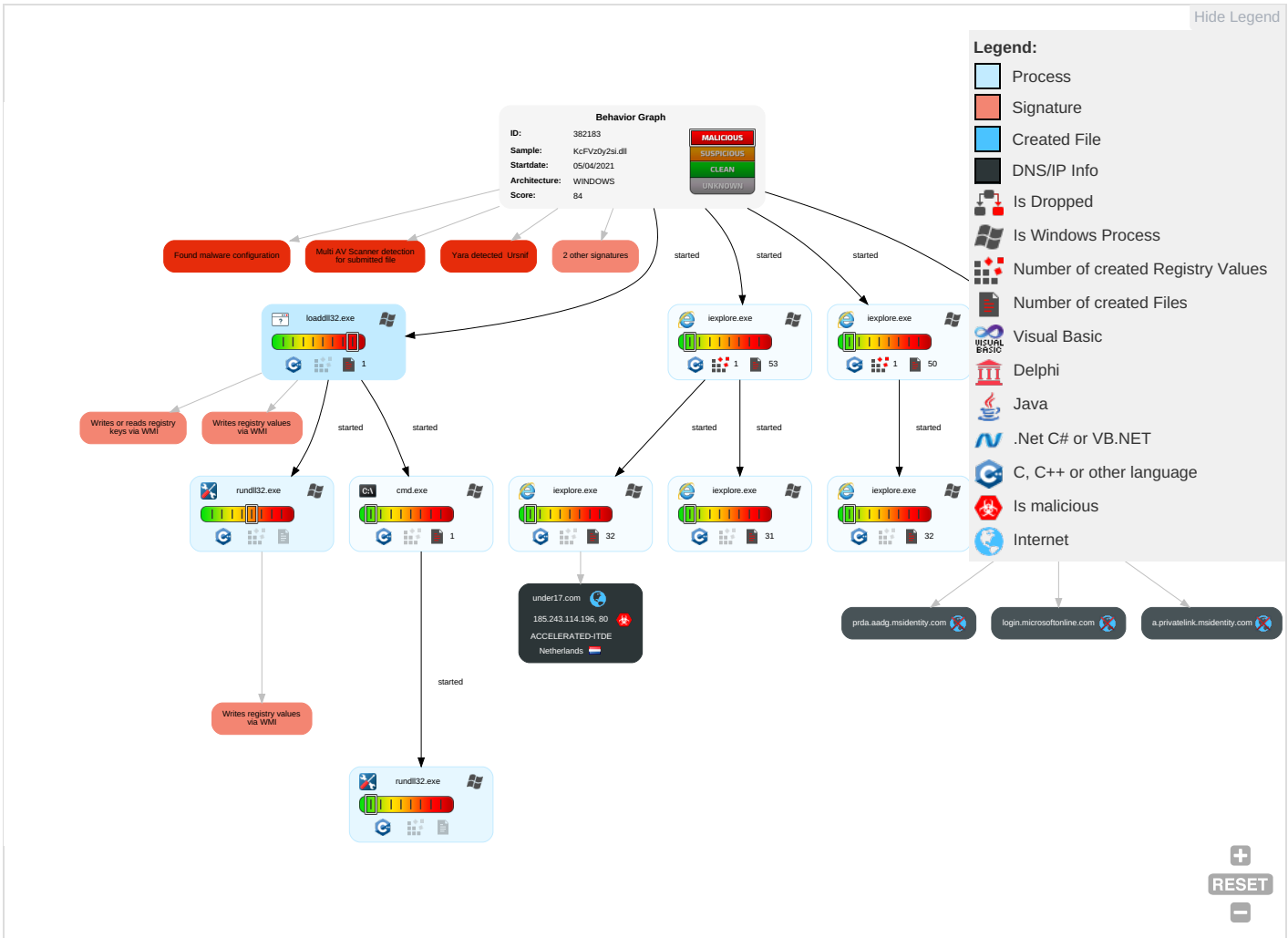
Remote Access Functionality:

- 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	Process Discovery 2	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	Account Discovery 1	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	System Owner/User 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	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

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
KcFVz0y2si.dll	52%	Virustotal		Browse
KcFVz0y2si.dll	52%	ReversingLabs	Win32.Trojan.Ursnif	
KcFVz0y2si.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.a60000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
3.2.rundll32.exe.4e0000.2.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
0.2.loaddll32.exe.2fa0000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
under17.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://under17.com/joomla/RnasiUAhJh/oSxo5X5EIKvwU8Ag1/uMFl7HC_2Fjl/9ltc89lzleE/s0K70MqQow8SbX/RmoUq	0%	Avira URL Cloud	safe	
http://under17.com	0%	Virustotal		Browse
http://under17.com	0%	Avira URL Cloud	safe	
http://under17.com/joomla/IlbeNmys4TdjSx_2FdVt/zKr90P9Hk_2BiF_2Ff8/DQfv4eLCQELbftpFrLH4_2/BewGR13P5J	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

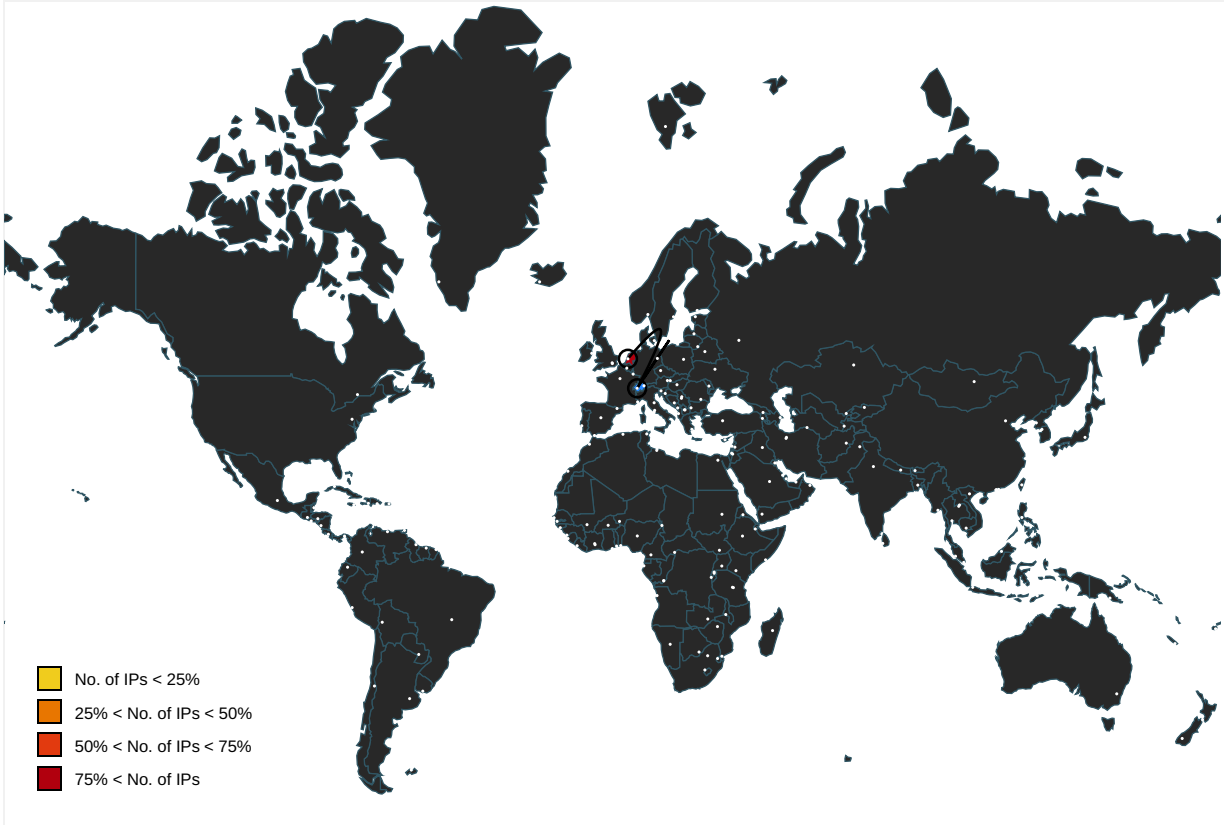
Name	IP	Active	Malicious	Antivirus Detection	Reputation
under17.com	185.243.114.196	true	true	• 0%, Virustotal, Browse	unknown
login.microsoftonline.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.msn.com/de-ch/news/other/inzidenz-vor-allem-in-istanbul-hoch-erneut-mehr-als-40-000-coro	msnpopularnow[1].json.7.dr	false		high
http://https://www.msn.com/de-ch/news/other/sind-die-500-wegweisungen-rechtlich-vertretbar/ar-BB1fkglv?ocid	msnpopularnow[1].json.7.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/vermischtes/querdenken-in-stuttgart-es-geht-um-selbsterm	msnpopularnow[1].json.7.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/international/zweiter-weltkrieg-in-griechenland-die-zweite-sch	msnpopularnow[1].json.7.dr	false		high
http://https://www.msn.com/de-ch/news/other/admirale-begehren-auf-gegen-das-verr	msnpopularnow[1].json.7.dr	false		high
http://https://www.msn.com/de-ch/news/other/bei-gebet-zum-ostermontag-papst-franziskus-erinnert-an-menschen	msnpopularnow[1].json.7.dr	false		high
http://https://www.msn.com/de-ch/news/other/gaga-regel-trotz-fallzahl-sinkflug-warum-steht-israel-immer-noc	msnpopularnow[1].json.7.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/coronavirus/die-neusten-entwicklungen-coronavirus-weltweit-ab-	msnpopularnow[1].json.7.dr	false		high
http://https://www.msn.com/de-ch/news/other/eine-stadt-feiert-ihre-vergessenen-heldinnen/ar-BB1fkih4?ocid=B	msnpopularnow[1].json.7.dr	false		high
http://under17.com/joomla/RnasiUAhJh/oSxo5X5EIKvwU8Ag1/uMFl7HC_2Fjl/9ltc89lzleE/s0K70MqQow8SbX/RmoUq	loaddll32.exe, 00000000.00000002.913123294.000000000135B000.00000004.00000020.sdmp, ~DF3D1717B6AEE1212D.TMP.8.dr, {D2E72914-964E-11EB-90EB-ECF4BBEA1588}.dat.8.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/de-ch/news/other/pappa-rechtfertigt-polizeieins	msnpopularnow[1].json.7.dr	false		high
http://under17.com	loaddll32.exe, 00000000.00000002.913202571.00000000013DF000.00000004.00000020.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.msn.com/de-ch/nachrichten/politik/coronakrise-laschet-fordert-harten-br	msnpopularnow[1].json.7.dr	false		high
http://https://www.msn.com/de-ch/news/other/vjosa-osmani-neue-staatspr	msnpopularnow[1].json.7.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/schweiz/	msnpopularnow[1].json.7.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/politik/konflikt-mit-russland-borrell-sichert-ukraine-unterst	msnpopularnow[1].json.7.dr	false		high
http://https://www.msn.com/de-ch/news/other/nawalny-gesundheitszustand-im-straflager-weiter-verschlechtert/	msnpopularnow[1].json.7.dr	false		high
http://https://login.microsoftonline.com/common/oauth2/authorize?client_id=9ea1ad79-fdb6-4f9a-8bc3-2b70f96e	{B87D9162-964E-11EB-90EB-ECF4BBEA1588}.dat.6.dr, ~DFB4B54F0F959EF8BA.TMP.6.dr	false		high
http://https://www.msn.com/de-ch/finanzen/top-stories/globalisierung-ohne-die-weltwirtschaft-w	msnpopularnow[1].json.7.dr	false		high
http://https://www.msn.com/de-ch/news/other/russland-putin-erlaubt-sich-selbst-das-weiterregieren-bis-2036/	msnpopularnow[1].json.7.dr	false		high
http://https://www.msn.com/de-ch/news/other/miss-burma-stellt-die-junta-an-den-pranger/ar-BB1fk4ie?ocid=Bin	msnpopularnow[1].json.7.dr	false		high
http://https://www.msn.com/de-ch/news/other/grossbritannien-boris-johnson-will-am-12-april-erstes-bier-im-b	msnpopularnow[1].json.7.dr	false		high
http://feross.org	GiGr-rA9TBhE2c3LJn7PvDweiOo.gz[1].js.7.dr	false		high
http://https://www.msn.com/de-ch/news/other/eine-woche-lockdown-in-bangladesch-h	msnpopularnow[1].json.7.dr	false		high
http://under17.com/joomla/llbeNmys4TdjSx_2FdVt/zKr90P9Hk_2BiF_2Ff8/DQfv4eLCQELbftpFrLH4_2/BewGR13P5J	~DFD254BC66F83ED0AF.TMP.11.dr, {E0E69389-964E-11EB-90EB-ECF4BBEA1588}.dat.11.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/de-ch/nachrichten/politik/wie-die-allianz-draghi-macron-europa-ver	msnpopularnow[1].json.7.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

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	382183
Start date:	05.04.2021
Start time:	22:35:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	KcFVz0y2si.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:	13
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@18/115@5/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 35.8% (good quality ratio 33.1%) • Quality average: 78.4% • Quality standard deviation: 30.3%
HCA Information:	• Successful, ratio: 78% • 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): ielowutil.exe, WmiPrvSE.exe • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.88.21.125, 104.42.151.234, 168.61.161.212, 40.88.32.150, 88.221.62.148, 2.20.142.209, 2.20.142.210, 13.107.21.200, 204.79.197.200, 20.190.160.70, 20.190.160.131, 20.190.160.130, 20.190.160.74, 20.190.160.9, 20.190.160.68, 20.190.160.133, 20.190.160.1, 40.126.31.141, 20.190.159.134, 40.126.31.139, 40.126.31.4, 40.126.31.1, 20.190.159.138, 40.126.31.135, 40.126.31.143, 152.199.19.161 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, www.tm.lg.prod.aadmsa.akadns.net, bing.com, www.tm.a.prd.aadg.trafficmanager.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, login.live.com, audownload.windowsupdate.nsatc.net, www-bing-com.dual-a-0001.a-msedge.net, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, www.bing.com, www2.bing.com, dual-a-0001.a-msedge.net, ie9comview.vo.msecnd.net, update4.microsoft.com, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, www.tm.a.prd.aadg.akadns.net, login.msa.msidentity.com, a-0001.a-afdentry.net.trafficmanager.net, www2-bing-com.dual-a-0001.a-msedge.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.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
22:37:08	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	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
	document-1590815978.xls	Get hash	malicious	Browse	
	document-66411652.xls	Get hash	malicious	Browse	
	document-415601328.xls	Get hash	malicious	Browse	
	document-69633738.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
under17.com	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
	document-684762271.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1590815978.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-66411652.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-415601328.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-895003104.xls	Get hash	malicious	Browse	• 185.243.114.196

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ACCELERATED-ITDE	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	document-684762271.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1590815978.xls	Get hash	malicious	Browse	• 185.243.114.196

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{B87D9160-964E-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7695506921153294
Encrypted:	false
SSDEEP:	48:IwtGcprgGwpLyG/ap8xGIpciGvnZpvkGoxPqp9iGo4VLzpmvGWx59ThGWx7T6p7j:rzZoZY2zWPtYiflVLzM3jJ6zXBcUpB
MD5:	8AB87F351BD1186B1248E0D7DDB93F07
SHA1:	9791E7CEC75F68490990217D65959B7891563D70
SHA-256:	712DFE38818E13B7137382E88F8A4ADCE096A16D7CB261AD4C46C5118BCC1F80
SHA-512:	9620D08B144614A0388FE0D6D307F7A169FBA552328A407ACA179AF6622706F21E4494D24F92E50EE1F245F0145D7F7F7854B2C1B2A138AF98B47DB276AB9B6B
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{D2E72912-964E-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	50344
Entropy (8bit):	2.000356934098388
Encrypted:	false
SSDEEP:	192:rvZUZK2WW4dt4zif4f8uzM472B4u2D4NTDcSNZCuM4cHZCuNZUtM4+6ZUt44NN0i:rRkpNAPBForHZTma
MD5:	CFE2A3DF4D83F27A1A1196C9227F2BFB
SHA1:	34C7C9D94EF9283E376C9E644863ECB87B2BF183
SHA-256:	365006BD57026427B4460EA88CFB9CF4F13D95BC3D140C0E276DAE55D0575737
SHA-512:	45D12EED86EC2C8C6FE4C73103BB8A4BE1848395523A8FC978F1C6F1E930C3719A21F4F9389C438685CA645C2243319064877A414E805A86F0F90634FC4B7C8C
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{D2E72912-964E-11EB-90EB-ECF4BBEA1588}.dat	
Preview:	.... R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{E0E69387-964E-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7691120184338767
Encrypted:	false
SSDEEP:	192:rxZ+ZkT2kUWkctkVifkdU2zMkAOM6CCBka1pB:r3qkqkDkok6kgkNkw
MD5:	654079C1E37BD8799BDA1715814F46D2
SHA1:	8EE0BAD603233E71903F3B0FEE24605291ABF193
SHA-256:	9E94FD38BC63CCAABB0AD23FDEE3494776AD0B7CD84B4124DCD7DBAE7BE635CC
SHA-512:	74FF4C1B5EA4515864341E03C837E020251AD736E0CCD55F6E801537BD33DE96AE9BFD2EFD35809F5803F6C22A1B18F4F502A07569DC43B150B07D383164F889
Malicious:	false
Preview:	.... R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B87D9162-964E-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	43268
Entropy (8bit):	2.503136716833044
Encrypted:	false
SSDEEP:	384:rAEgIugMrtk5t5Wv5n5B5K5TfDPfDB5AfDqbI5gN5v7:hDXDKDS
MD5:	42DAD9E72F22CCE29E7A81F3387A4416
SHA1:	145F5C99C2CC18FD79D05BB7553869F66CF1EA78
SHA-256:	C5FBB37C42BDE558594D54B20E467D7E91494AD2DC62CD0962C2C56A6D49614E
SHA-512:	7999A3F35F6812893287079F58BC88995E6ADE6F3E29B0FEAFC34BAB37006292D9A8AE9FE0F9D337B92184FD49734005250D75F68F28AB4B2F83EDFD011646CA
Malicious:	false
Preview:	.... R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{D2E72914-964E-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	27356
Entropy (8bit):	1.8407671824667158
Encrypted:	false
SSDEEP:	192:rWZpQ06Gkzjx21WvaMmu4AWsR4AWgAWMA:rSOfH/gMzRs0skn
MD5:	FB6BA55B9602424F2BCCA7D6D56C571A
SHA1:	95E1983B509D0809091C66A463F4A06FD3A975D6
SHA-256:	11C8C1C5FCE8BE80F6A2F532A71DD3D95FF585531136C4DC3AA90FDE24C6F799
SHA-512:	27C7A6343E5717305C39623A44B613F39C86B61FB30C1DD7881E8EB240C1ADD8393A014576D4FB7C7A9C6BE0B4F73819D81936D2948B9117494DAFC5108D886E
Malicious:	false
Preview:	.... R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{D2E72916-964E-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27420
Entropy (8bit):	1.858875120868889

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{D2E72916-964E-11EB-90EB-ECF4BBEA1588}.dat	
Encrypted:	false
SSDEEP:	96:rGZdQx6/BSRjZ2tWGM6uOkuXkLOROkuXkMA:rGZdQx6/kRjZ2tWGM6u+lR+XA
MD5:	65E5372483242604D285C40F02317089
SHA1:	7F3470BFF16CE5C6D8EC5693DBD6A1A604F830B7
SHA-256:	19FFE8E5F373B6C70D33780E5091DCDB9CE42026F19C81DEAFDB6FD48E3C659D
SHA-512:	510EA639F919464BDE91FF271F9DCB8FF081DA155CBBED1EA0707B5943B130AD5B03DE6156067FD8B1308A30B02667379E39BC7ACBC90C37DCA2245932B7D15F
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E0E69389-964E-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27356
Entropy (8bit):	1.8396751565777196
Encrypted:	false
SSDEEP:	48:IwdGcpr0GwpasG4pQcGrapbSY1GQpBuGHHpcrTGUp8CGzYpmktGopsi9EIX0j6s1:rDZMQs6aBSej92FW+MWu4h3jR4h3ShfA
MD5:	48DA3E58A0A71DC4D6C504CBBE0D02C9
SHA1:	7371D5F4B2546F0B25545CA4562C03A7AB63CF4B
SHA-256:	3DCCF18BBAD110F20CFD668B4186FA8FA71B1116559228CF411919A8AC543765
SHA-512:	808DF87721DF4DBA63551C32E2B6AD220EF80F9C13B7BB47104AC7080E24569A2E5B028FF7A04ACC3227D958B361CF7787B693170E816632ECC9700ADAD9142
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	5096
Entropy (8bit):	4.535210143895889
Encrypted:	false
SSDEEP:	48:wXLBRh+sCBykteatiBn4KWi1+NCXaYgDehYa3DCW:0Ph+Qhato4xfDehrmW
MD5:	9632B6DEA655CFEA1A0FBA407A57A8A5
SHA1:	FDC48ADD56570B72FE067F26C5AFFBD2771DBE99
SHA-256:	661E10AA9C474C7370D530320FBCCA11DA53ADBDDD2417C025FEB7F837C2B91C
SHA-512:	FC52FFBFD86F50A59BC7147B458477E0B462F79F004E31C8D850AC1AFAE9005DCB42CB2AA1EC6E3B7613399DB7A32849E83F98575D44A43494DAA0A25498255
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\2WF3MMUU\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/3HljKR99U1TrD3ptYZ7GDlh6mI0jeI4dIwDq8rz:rn1edcjg5pm/IKRXU1TrD5tJf6mzjidJ
MD5:	6D8EF11CB1C03B39D9ED4E4C9A2190B9
SHA1:	265DAF51294422A5A393EF7D32E629E16EF8CEF4
SHA-256:	D72BEAE30A6B2B36C3E03847CE4EA04211D7373D4066FF937A7A05DF4E0C3DB6
SHA-512:	C8820BDF2FC34CCFF7018A1C1E3E74ED1FE0B287926050F9B6BA59C08DCC216E8732F862AB0BF086BC05275C51E6F81132AFA60F6D50A19585642BC906DCDD2
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/Jl2vUSlEIqWjk-99MuYp4W74zvQ.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\JI2vUSlEIqWjk-99MuYp4W74zvQ[1].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 1.34 824C2.23985 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 13.6 569C3.46197 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 12.4446C15.5 308 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 5.04104C1 2.1673 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\2WF3MMUU\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\2WF3MMUU\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
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 2222222222222222222....."....}.....!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\2WF3MMUU\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	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

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ZcieD[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):	372
Entropy (8bit):	7.358154316594694
Encrypted:	false
SSDEEP:	6:Xtb9leJyvoxsMop8K1HAKAq+0+BOUuFicJlZtEMtoKKzL7P1Ge8tRh/YDrdqz6hz:XtHIywWhV19+BOUuFicJr6MRSLDa3sBv
MD5:	0703C93C07D9BE0EF67F910F2B2A63F2
SHA1:	3C3CE7AC56C190662E991B10FA2B15DC12F11A8C
SHA-256:	CBE7117C62F714B48BBAA1D5244AFF13D0384EF3E3ED8AB95145E251F6EA7DB5
SHA-512:	58043F0C47E8841886D90F4B19B576A0AF2BF8EBE1DF34DEFC64153A510B2D4154B2FD901D8D63D88BD7FD1316BD86022C5938644FC33C61FE1978CE39B9E82
Malicious:	false
Preview:	.....T..R.0.@.....|m(P..w.B..''pG''n:)...`....;..n..98.M.....5s...d....0.2..F..s{.s.....i/..8.....J.~Z.O..o.,k.%.MMa.E.....&-K.&(..`.|...V.I... .g...A.!..Q....LP..''e...:.....<...j..El..)...%0Z..-.~ZE.....v?./....zD...z...x:..Ez.S.B..6c...g..&..~\....}}...X.HB>....V...C.f}ZU.%'JM.{.\.....h.''.2.C..<....3...Y...;'g.a.N.C....Oe.?kno.....8.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/bLULVERLX4vU6bjspboNMw9vl_0.gz.js
Preview:	0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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....#+....I..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\2WF3MMUU\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\eRYlUYIMYsB_Pt8B7FTik-pl5cs.gz[1].js	
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\2WF3MMUU\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
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\2WF3MMUU\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\2WF3MMUU\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\gDsOfTXNZVl18jxNDvhXqAdf2tM.gz[1].js	
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\2WF3MMUU\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\2WF3MMUU\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\2WF3MMUU\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:	downloaded
Size (bytes):	15963
Entropy (8bit):	5.525813716514189
Encrypted:	false
SSDEEP:	384:HLIePm3yt9YYr+RR5bV5u5hOuKsVMhu3kx0m4iDewY/rfrEraIO1uYPW:8Z3yjYYM5uTOuKsV2u3kx0m4iDewY/rG
MD5:	366973754B9073EDF309E3D3265EA893
SHA1:	FD59DC768CA91F9E377C2EC9606CFF3826A520D0
SHA-256:	7D140A0AB740B59EE540F29B152216E186E32B78200188953E1BD42A7EB4F134
SHA-512:	0EDA6E25AF01007F378F0BFD0B8C171F9EBE75D731641FAF8E39DBDE8C27EA1728ED67C6ACEAEE691A70B6F4830BB788C3DFCC8CF799B83B4F76D74B5FBD516C
Malicious:	false
IE Cache URL:	http://https://www.bing.com/hp/api/model?form=REDIRERR

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\model[1].json	
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":"2021-04-05T00:00:00Z","Iotd":0,"Dft":null,"Mvs":0,"Flt":0,"Imp":2},"MediaContents":[{"ImageContent":{"Description":"This stone bridge, known as Saut de Brot, looks like it.s from a storybook, but it serves a very practical purpose. The bridge connects walking trails on each side of the Areuse Gorge, offering safe passage to hikers exploring the Brot-Dessous area in western Switzerland, a mostly French-speaking region of this multilingual country. It's not known when the bridge was built exactly, but it's thought to be a recent construction.","Image":{"Url":"/th?id=OHR.SautduBrot_ROW9659507110_1920x1080.jpg&rf=LaDigue_1920x1080.jpg","Wallpaper":"/th?id=OHR.SautduBrot_ROW9659507110_1920x1200.jpg&rf=LaDigue_1920x1200.jpg","Downloadable":true},"Headline":"Info","Title":"Saut de Brot stone bridge, Areuse Gorge, Switzerland","C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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):	10448
Entropy (8bit):	5.499688432928685
Encrypted:	false
SSDEEP:	192:MdnU6GG392gM+XgaVCfELUuQkJUvImz8sZBaZv3YXi5Y9h65f73K4PUVK3ipMZjB:snBTIL8g+CcLjQAWdZZBa5IXiSneTa4f
MD5:	F13CE83C16A3CF49C80D460642C0A98D
SHA1:	7402C45E4648D97DA338D63342D36FE05BD8F68A
SHA-256:	2A917DC9C1A1DB66AEF4F850660C83AA1FFC9699BBAD327146DBA3ABF216C870
SHA-512:	90DE8EFB3534D7D6F39914579494852E3B5C66BFF6C3FA7E0E7039FBF9BA6133596455A66DA87A1D0466E4F74AABD59EE5BC03E8695D70C71E2BC2DE7F7DF576
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/eine-stadt-feiert-ihre-vergessenen-heldinnen/ar-BB1fkih4?ocid=BingHPC","imageUrl":"/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fks8r.img&ehk=MqQZgZrj4DCNtpVl11d0lE988SsVQ%2fcHQ6mTM6D%2fYss%3d&w=150&h=150&c=8&rs=2&pid=WP0","shortTitle":"Tages-Anzeiger","longTitle":"Eine Stadt feiert ihre vergessenen Heldinnen","accessibilityTitle":"","subtext":"","isRecommendedNews":false},{"url":"https://www.msn.com/de-ch/news/other/nawalny-gesundheitszustand-im-straflager-weiter-verschlechtert/ar-BB1fkpLh?ocid=BingHPC","imageUrl":"/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkpJk.img&ehk=HiIriPbRsbFHpW1R13YXE4bkulV96V5SFczX3iTffRg%3d&w=150&h=150&c=8&rs=2&pid=WP0","shortTitle":"BZ BERNER ZEITUNG","longTitle":"Nawalny: Gesundheitszustand im Straflager weiter verschlechtert","accessibilityTitle":"","subtext":"","isRecommendedNews":false},{"url":

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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
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\2WF3MMUU\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=B119ED207A0348168C3F1966042F2BFA&form=REDIRERR

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\sbi[1].htm	
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{display: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 img#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:grayscale(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\2WF3MMUU\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
Size (bytes):	4522
Entropy (8bit):	7.897730804548622
Encrypted:	false
SSDEEP:	96:pPE6XLVuyFxKvu2ec6CL3iFCMXNheOHtMD2On4ZlwqmuXxCGRD:pP6y7Su2caSvCIro8LRD
MD5:	CDCA016DBC4022E03D47D550D5853310
SHA1:	0A471FE54D10259BC4D4E1F77D9EBB12720B1A5A
SHA-256:	84521BC94352C824783093DED8E6B3A0ED26E155A185BBE99D9D87853A0CEAFE
SHA-512:	2338C3530E98185DCB3565AF55BFCA21098E4BB31E931AC874052EBBBF2ABD031B79C3588561BA99713FA528EA76D867200C49D82E63F4E0C1DB06E38ED461B
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fk8Fr.img&ehk=7HDLCHip4nqvrcbKLv%2fwBAhaCBrgofZotMuSFlq4HEc%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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....T...1...4.O..8R.....uMk...c...ex...55..g..]..7.'...j.f.....#Y.I.S..%..k.P.U..~.R....~ob..Z.k.....s.jj..)....o.K....=8...G.k.Es.)t.h|..$.x .Z?....H...T....P....(..A..`..qk....#...W.O.....k.....U.4.[.q...ZkW.O.G.V..i..y...1.P..J.....u^..T.....d.n...t..4U].Y.J.h'..Y...3.s....p.....v..mBY....3,.6B.g$.....J...).Q..z. ..QU..6..p.....R..\.D....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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):	3523
Entropy (8bit):	7.863527779206926
Encrypted:	false
SSDEEP:	48:5yYcuERAWjLzWTi1bHPDRGolg83Z+ZOHeKMdA9t3kZoIJDOZMH:5PEDCTi5RGTZOHP9aZoIJKMH
MD5:	46AA37D9E84064653C50FE5690208E99
SHA1:	56AB35A405CFCE616C62C5D4F832FD2569E463B0
SHA-256:	7B7F40955B5075CA6C2A5AF001B4D581F4980EF5865CC80A25DB240FF8CBE886
SHA-512:	F5EB0D32EEDD7356FB7FE6D10780493C011FE2310F3B8CBBEC05A5398C70DBF6270B172DFB77DB7545B5D615F39DFB2E51A4E68B46C1026F07A5F9D98872BCB
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkl4p.img&ehk=BwvZQElg6XeIBCYOPqnT0vlZfxZBSkm4G9lxezek060%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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..,.Nk~.A\..:.....;.$.o...?.5.tO.k....$...+T....j...h.\.L.0..d8...)I..n...L..u...k.Y~z..e.aR...Y.5/.h.\.E.2x..M.., 4{..U....+..K..*.....w....I.bkJj.KRI.C.u".....UY..U.Q..#*...{.p)..y.....Q.,.&...9,j..d.Y..G\..[.v..1...j...B.?...F,.nm..0Z...nX..W^w..QHN.N.r..]...+.....{.E....pz...k.O.kR...wY,r.(l.}..jl.T-.2...V.T..hx.E9JLh.L...~t..Kz85.p.54...*.e5..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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):	7484
Entropy (8bit):	7.9386500897510315
Encrypted:	false
SSDEEP:	96:pPETdSD/no9uqn4iL7VWU2n4/2oOO4S56FuLJUSr9JKVtdPq1NWWk4nYcaBh5J0J:pP6SD/o94iL7N24/2oL4SaWeONWoLjJ
MD5:	B4E79D9AE9E97E8C04CA32DAE1EA4248
SHA1:	E21331D7E5CB397512B99D83C2F1D11EEFBBC550
SHA-256:	62AA54FCF54AB16C95C616CAC8AED3DEB545B2B7D1F0A26570A59C257C8B8645
SHA-512:	A13DA8C11E232B664864625B10360A5F08B5C4143BF5A26AEAEAC8A917B6B96DFE85F642FEF8CB37F6CE5CBD9230D0453E41563403FB8B749B932509A6815B4
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkbU5.img&ehk=wSFsJFJNi7w9uIvT8y58gYoDbHASimqWpZCj5GfaXgg%3d&w=150&h=150&c=8&rs=2&pid=WP0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\th[3].jpg	
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....4..\.3.!...d...s...4.....a...=Q...zW.<?f.HX..\.Q.^.9....p.v# t....sN.zn?.....I.z{T.e0...0<.&xA. .?...;/._.V.<..{.:.0...2.t..i.....2J.n.....3..zrG..NaJ.l=o...)9.p../ .r:.~...~...m.....C?.$...W8@8...Z..46"Qq.-....'..i# .....kBF.....NF8.]....t..m.E...O..T.....6..Rz.0i.8.".[j...I...&=8...i....5+t...El.)=..q..?3}qVf.F..FU..u.q.....f...r...r.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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):	5402
Entropy (8bit):	7.9124610392559065
Encrypted:	false
SSDEEP:	96:pPENXBviLAR2EbjBbYztUfMzC2UtlKNiWUXe+N/ObihjoaxZk5NyIIRqfYHS:pPWXFiLABBAtuMfUtl6UT5ObmJxZk5EU
MD5:	331D153A161C5BF7DBC08E7A9E433DD4
SHA1:	849F965F11F5889DE5237A9545502A1EAB90C709
SHA-256:	42C0722BE23C91E31E16541690D55D5DBAF877E1C1AE363A827B806D413049E9
SHA-512:	0DFCDB8EBA0DA7B02051169478EA943C93E6CADFBD7F4297C417F54ED7CA3D7DEAAC78D1BCB83118F40E90790983A57D68DCB22FFEDA43AEECA96C6A97DE E997
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fjAOq.img&ehk=H62q3CZ4wZ9m1QkcogrP9%2bbfVUrHILv2KztDdiMBHGc%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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..G...NI.E.i...J. x.i.n(g....w._zh q...\7^*P@.)...s.....^.A .....E..J0... !$.$,..N...f.[[..t..G..y.(.V..c4.X.y.....Q.....&...i.M $.`/N..2M<...+.1E+.z.L...A.....~Z .$..4.yr}iNO4..(.@.....N..L].`.L.#...K...T...."..|.....9..D..Nj.#HT...$.f..Hd.z...z..1.*...`w.i.y.S...NU....O.N..z..H.6....Y..2x.o9..S:db..}....b".fb88.).q..@.pr.i...P....S..`N..I..3.z..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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):	4949
Entropy (8bit):	7.908321794025412
Encrypted:	false
SSDEEP:	96:pPEnQ5IIwkMduHEY73tdu8lGyo8QuD0oCRTMfv:pPGQdMduHEmfuQGx8QuD0HTMfv
MD5:	EF6AA0C021E943F3F3C4188A71C49963
SHA1:	5939DABBAFDE6190256D76FF8BF152855C1EBFF2
SHA-256:	89AB1DCAF4F9D67FD3BE873BDFC384A42CA8B09DDAFFA650CEB18FC2B47CADB7
SHA-512:	6A8AAAB26A6CCEFCBF158A16AC5508F4971F2A837428E9B5F0617ABBFB1E1022DD7EC30D0DEB3EE35E95461D918484DCB4A4DD2D61BDCC3904E7F3BBA55D C20
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fjWtX.img&ehk=LAmTwTbmDq%2fCHKWjys61HZFZkl0KC3r%2fHMfSOeyLBDc%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..... .....?....b.c%."..).....i.li...Wp>._N.....3P.`G"..GN+5.!...z..ub.6.F85S..hp..H.f5....0...T..q.H.dX.....*Si..H.....j..n.[.c.l..f.n.cd).>.5...A.OZ.S.4.3..@..R..R..\& I.*x..r.{.i...T....j8<..q.k.1\.:.n$7.....DJM...r..G...~.+JXC...z..Y.R2.Uy].$g..v..\.&....D.R.M..=...L...W|..../q.X..Z).....}.I..T...V.....x9.[...ls3/.~.S.....L..LY.5..'"95..6.2&..|...~u.s e..[q.W9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\4L4QdyjTv0HYE2Ig2ol9eYoqxg8[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1101
Entropy (8bit):	4.829151166001716
Encrypted:	false
SSDEEP:	24:t0S8eLfl954T0u2y3EO1gRcDrIvQaDxijjfscC:vLfRWtPDuQKIjq
MD5:	91CD11CFCCA65CFACE96153268D71F63
SHA1:	E0BE107728D3BF41D8136220DA897D798A2AC60F
SHA-256:	8EE1E6D7A487C38412D7B375AC4A6BD7E47F70858055EEB7957226ADA05544BE
SHA-512:	4367CE147C7FA4590838F23C47819B8954858128336979E28BA116924B92660A7CBDC9A8292C45C5F26FF591F423F03DFADCB78A772DBE86AC5FBABF0B4E7711
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/4L4QdyjTv0HYE2Ig2ol9eYoqxg8.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\4L4QdyjTv0HYE2Ig2oI9eYoqxg8[1].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\9026IKNJ\5rqGloMo94v3vwNVR5OsxDNd8d0[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	461
Entropy (8bit):	4.834490109266682
Encrypted:	false
SSDEEP:	6:tl9mc4sl3WGPXN4x7ZguUz/KVqNFvneuFNH2N9wF+tC77LkeWVLKetCsYuwdOvX0:t41WeXNC1f3q/7H2DlZWYeIsrGYyKYx7
MD5:	4E67D347D439EEB1438AA8C0BF671B6B
SHA1:	E6BA86968328F78BF7BF03554793ACC4335DF1DD
SHA-256:	74DEB89D481050FD76A788660674BEA6C2A06B9272D19BC15F4732571502D94A
SHA-512:	BE40E5C7BB0E9F4C1687FFDDBD1FC16F1D2B19B40AB4865BE81DD5CF5F2D8F469E090219A5814B8DAED3E2CD711D4532E648664BFA601D1FF7BBAA83392D3 0E
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\9026IKNJ\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, precisi on 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:	3685F5DD0B8869A0B71C4CADF4FE8559094DC431FEE1E14C349BF6E933702B90136EE45277A97627F69BBB6FAB5ED9EF98AFEBCF88079C5EFFEBD4100B64CE 21
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!.!2222222222222222222222222222222222222222 22222222....."....}.....!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\9026IKNJ\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, precisi on 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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\ELqKWpA6KkapLUFbOLS-IQ2zfXc[1].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!.!222222222222222222222222222222222222222222 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\9026IKNJ\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
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\9026IKNJ\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\9026IKNJ\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\9026IKNJ\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\9026IKNJ\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:	CA0EB961E52D37CAA75F0F22012C045876A8B1A69DB583FE3232EA6A7787A85BEABC282F104C9FD236DA9A500BA15FDF7BD83C1639BFD73EF8EB6A910B7529 0D
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.bor der="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\9026IKNJ\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:	69F8A2161EDE8AA0BE70ECF641D1C05D7E9B5E6952DD41255E02B7AE9FAFDC94A9547DDDB46A2FF9A56C852239558E3C6634D93A1D6D7669C719956C8D2F5D D6
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" f ill="none"/>.. <path fill="none" d="M0 0h20v20h-20z"/>..</svg>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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, precisi on 8, 160x160, frames 3
Category:	downloaded
Size (bytes):	14848
Entropy (8bit):	7.9161237402148545

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\b4Jy0kwhnsWcsDQyuzAEsN7RmhQ[1].jpg	
Encrypted:	false
SSDEEP:	192:d5KKqPy60pSDqRxY0cKZR+dG0cDizbS4z0GoJmsrod96rIE1KRCLHXl4DPzEmISD:dg9PJvoe0LsG0iiF+TVERCjgEmgDG
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!.!2222222222222222222222222222222222222222222222222222 .....".....}.....!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\9026IKNJ\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\9026IKNJ\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:	EB645D1FBB404B00D19C743C3F6F00597D91DE73EA2F02AE61AB76AFB13A913F68CB2419C205684CAD827D1369D8F76D9B7E709B8EF0AB05A86B305A7A5B7089
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\9026IKNJ\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
Category:	downloaded
Size (bytes):	1567
Entropy (8bit):	5.248121948925214
Encrypted:	false
SSDEEP:	48:KyskFELvJnSYVtXpQyL93NzpGaQJWA6vrIhf7:KybivJnSE5aU93HGaQJWAilh
MD5:	F9D8B007B765D2D1D4A09779E792FE62

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\n8-O_KIRNSMPFWQWrGjn0BRH6SM.gz[1].js	
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\9026IKNJ\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\9026IKNJ\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:	E85360DBBB0881792B86DCAF56789434152ED69E00A99202B880F19D551B8C78EEFF38A5836024F5D61DBC36818A39A921957F13FBF592BAAFD06ACB1AED244B
Malicious:	false
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.bindToConditionalSignIn=function(n){sj_evt.bind("ssofirstquery",function(t){return i(t,n)},!0,null,!1)}})(t=n.ConditionalSignIn||(n.ConditionalSignIn={}))})(BingAtWork||(BingAtWork={}))

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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:	D3715E6A3C9012F2D8E1269E5C4B3E2F77FD2CD8E793AD39E51F1E1BE30F0818DDD01FAF3708EF789FDF347B92C6477C10A1155DEC582FF68185CBFD41C662B4
Malicious:	false
Preview:	IPv6Tests.TestIPv6Response('{"type": "4"}');

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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):	6668
Entropy (8bit):	7.93390698549457
Encrypted:	false
SSDEEP:	96:pPEonFJa55jLOZYwc2x3mh66yiIgnyla2iGSZlaupm8yQfQczEWXHFfuz:pPhJk/SYwLI3yitE3ckupxLQc4+BE
MD5:	16FBB0D8BBC962139352C3B628B1DBFC
SHA1:	4E8CB16861A9C7E2C21436A65D360B2467A4D25E
SHA-256:	4A20F4D7EDA4224CEB5FB07A802FEA997117AF5FBE99CD1038478AC9A49A47D7
SHA-512:	0C91A10F8350233DAB0C8CABABB41BB10F7BD8EE7C147DAB597E2FCECB2F34619196141F14C166F52667B5D1AE354FA24908DFDA31B07BC43616930AD16CC1E9
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkhKJ.img&ehk=O0D4ivaDhx74SkRSyKWmYofxh6bf9w2kbNeWXmgUoBU%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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..@.K@.....b.E!..)h.,&(.-&(...R.8..`..^..;2.ls....8..?.m...2o...,...*m....jC.E.....`..m...a...y..`J.*@i.RF..c#..@iR..iji...+5..Q@.....u.....l.3.V<..m...?.@.L`...Z.{..E0.d..k.n.....$..{.G....&fTR]..3..)k...mR....p..JW.6~.a.=.k[w5*Wcj..3M.&j.?4...Fh...ni3@.....M.F}gS.N...=?x.T...X:.'X.y.?...6...4.h.0..)..@...h.....8.*.8..9.....%.H...=Y....s..S!..%vh Ix1.$(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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):	6086
Entropy (8bit):	7.9329147945603316
Encrypted:	false
SSDEEP:	96:pPEBVpaWyiMCTi58el7n8yJsVrEciIRKA/7A66KijTlLDiFzZPI3iVsXHBrS2/:pPlVsWyiMH58mnfJcrNKA//0tytP8VGS
MD5:	324B650878015266D0F8293847875BE9
SHA1:	BA179D63FFE16867F104EC15CA49B5AD5B871C01
SHA-256:	18C4E511572C6EB8515E0A7685CCB9625517692E81DA600BB135D338850C3F01
SHA-512:	41117D8425CB010501C8FFC48527B42383B74452D0B2D3A9A9872D19BF8F57BF0AB9E1D5B4A7D4D93545D20091355872FB131C697B29BD8E349586A8C114563D
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkcOH.img&ehk=wP%2b5NSDmh%2bsJZNE7v2A1A8SY0I1I2EGcaPxI6kHo68s%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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....>F]...;=.x....sR\.'.F.6....u...7.1.|.....6g>ZBO..2...J....4...E...s[.....t...H... Mr.a...g...e..kP...2..p+.OS.&..-.J...$...N9.....m...u...4p..KGA.T.u.0.....k .....q.s.\..e.(..#5\.2..w...C.M..c.Ef_q...L..R9...~a.. G.Wj.?$.+b.....$....!6....Kh.<.d.....l.....m.f&;.=~..qi-..,....9....@.$...V.M{..../d..U.q.....b..?.*....^..i.2..`..5Z.O..c.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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):	8935
Entropy (8bit):	7.945942030509575
Encrypted:	false
SSDEEP:	192:pPXVvHKaC6qw1yvBdEjI7fo8QQ5UHzZR8TJSOxS:5tHV8vTUavQQ5UH4VrS
MD5:	AB4F28F6751029B5BAB54E0BA4255026
SHA1:	9425F8DF6A33276B371656C66C47AE0B89DAE774
SHA-256:	8DCAE4BEC6B1FABA277F53E486DCC49E18E6538597B7F4DCFBBDDE2DB1067AB9
SHA-512:	10801B62C6AD34A38A1356C05EFC6CAD95A8903378AA75452D510D9A1DD8C6AA34E10558F8E44E98B5D7175CE8752E8ECCAAED2962A6D95C70794C3C5B2BF07
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fiX4I.img&ehk=oAAZIiXj%2fumZECw2C5kUqivibA8UChPv16TWwkPuhU8%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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...sJ.$...._..O....h...(.1.....8.9..Kq...x... .-...*G...cXBc.....s.y.Y.u..u.....k.[l.p.d....^I...t.9..j9w...v.x.#.8...>....d.V.M+H.+3<.9.B.NA..;g.`.....]zUK.R.N...d,..O.u?.ye.....R./.?...._.a....98..1.sH$]6..=....K.....A.7[.....k....$1.]H..X.+.....J..>!...`..W....y..v...^..\=....M.....!..72...$w....O.....%.....c.j60.zg.....4.QF..FxT....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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):	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\9026IKNJ\th[5].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):	8011
Entropy (8bit):	7.94253125941382
Encrypted:	false
SSDEEP:	192:pPdZWYPb/28xEIkwltQDclRW4jPFSVzc5T5plxdDeO/6mgkOTCS:51TnxEIkwltplX4c5T59d7gRuS
MD5:	840912C74FB45355650821BCEA88175D
SHA1:	93C37AC08B89484F701058423F4DFF5420EDB633
SHA-256:	F0EA1E75759C741C3D94C1844877D0C34D45B4DFD2D4E4F5ED4FF50AAE3727DB
SHA-512:	C998AAB7DEF08ED52BFF6349C214E358A29FCA56377FD94E6A52DCC0D39538569166E22C6424E0468CD3988E7A3529E9E3C4CC4D46083610FD7C505361C5054
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fjQUM.img&ehk=ohGTsOxHGMO2cB8vhDGQrLDHJqHlJQ%2fve%2fzuz8I%2fuRg%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..... .....?...4.....1.Y.Z.t...L.Ej.. ...p.}..2.KH.....]yd..A...;..5..Y]m..k.4.a..rN#.....4.%...."8.....,b.J.FV.V.....@_...Q..gM..~..q.6...&.Q.3.Woo`.f...u\...e c^:...Z.H...gg.>...E..?.k..._I.&.....&.....?.Ci;...<..7~y[yn.....1....x.Z.,...ai.J.p.v.a...[..t..v....h.~..-.....4..zg&.....Q.H.KF.0y..=y..V...y..". nS...x'.v....z..+.OZ.....y8...Q...Z+M

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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):	6093
Entropy (8bit):	7.927239270981086
Encrypted:	false
SSDEEP:	96:pPElGyMvEietDQS5a27K7DS0p5xLLflVCa+yfBTCmLekx/QZ0KJ6Nd8bM0U0IsdM:pPhyietDQOaY90pvlVDHdekpK00qoDI9
MD5:	E9906EE547BE715E8F684E65A73D7EC4
SHA1:	BD86DEE901B1C0AEC9A3D928DD2AAE8936AF8465
SHA-256:	C3623DF3066E6D08A89D322DCC883A2CF2CC59F61D23B6D0E6EFE7F08F3705D8
SHA-512:	F96164274A46721CE997045568FD82E2A05E1D4D73E53002A5D51F46969DC61B52A7F70EC5D048F6EE57EBE3EA74A37678B0E4E31F2D29CF55449B5E195D09EA
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fjZJK.img&ehk=QDs%2fHMyF5PcvjWAKFYIK9ivMZM8fXzByzjyjg9niFV8%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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..X..3R}.)..R.....5...A.$|..mi....g...H.W.....s....h.n<..bBx....iJ...Q.....F{.G....A.zw.SX..#2Y.q3.....).}Oa.Ro.L$K..U.....,2,C.j..../)?..<....JvdJOd u.V.ZZ...+....$....\.6.....&..Gv...._>RW.A...X.c.m-....?..[!SgCoymy.....\.W.D.....n..\Cct....C.....,-....%..~M.....Q...u-$$w;.s.8Y.w.a..Q..{...A.T...#l..x.8.C.,v.!*...$>..(H..{.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\th[7].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\th[7].jpg

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):	7609
Entropy (8bit):	7.926954037737342
Encrypted:	false
SSDEEP:	192:5P+fohx6+mHxIrj4KaB9hoNLt9SicDPs7CYt/W:J/hmHxIrj4KahoNR9ADPsx/W
MD5:	26FFD3C0CA11533F5B7A3F3C0A8BFC44
SHA1:	DFE845981D14FB0E668FF7D200DAAFF8F3CDCCFF
SHA-256:	AA5E97EDF16ADC1DD1F61256E187935B2F0F598E33590A61148DE94FACEF4ED0
SHA-512:	2B8D91E7B0FF19685A0BB71CF19A25E95F3B00D21ABCDB7B9C8E50F87A565C6CF979FD30D1F728E115DC12DC2A1D7D01AB5D579F731D6D6A8AABD637C5E95AD
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fjThq.img&ehk=jDUH6pgLukqRD8%2fPLfIVmzwP%2bdszXZCVoC%2beTw3gNyE%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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....S....qN...u$P.`.p.#q=...Z...m9'..*,...U...@..f8...s..=.rj.V...$.....w=?Jv..o....3PX.}..K.z..S....h.}..E.O.....w.....P=I.P..^3.j,0....oC...u.*=R.@i..4a..#..(.%2Hz$hX.B....?..{....v.....:.9..(7.Fv...&.kz..# V*x .....i..|.0..a.....-H.....W..Y*.>.../:..=U.....y...H....Sk...(K.V$.....,_.t.....@....v._.a.I..R.{.2%.b&J.R.c....5...q.u...*@.....{.y..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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\CS6IXJW6\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
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\CS6IXJW6\HEBN3BKD.htm

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\HEBN3BKD.htm	
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	60533
Entropy (8bit):	5.761569884404903
Encrypted:	false
SSDEEP:	1536:GUrSCXrLQvo3HJmcpUQlETOuKsIecFXdAjvdC94fJLYvD14eb097Q53Opw:GwLQQ3pdmQmdC9Rfew
MD5:	E9334CB67A6DC88AB86C004980AA4A92
SHA1:	562F16072E898601D092C5870C21BB9F4D5F2BE6
SHA-256:	C64C5D6A03D4126DADB7044BFD9E979DB2A051F7ADAAD3A3C2EA8E13A3AFE01C
SHA-512:	D9642547DFD013DA596F1E8A1660D10FC72977A791AA456A9A1DCBAEFAE929958808281742FBFBDBF6997EA9E20ACC52A1D0BB2A288ED0A5420D2EFE3B971A89
Malicious:	false
IE Cache URL:	http://https://www.bing.com/?form=REDIRERR
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="w idth=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.SautduBrot_ROW9659507110_tmb.jpg&rf=" /><meta property="og:image:wi dth" content="1366" /><meta property="og:image:height" content="768" /><meta property="og:url" content="https://www.bing.com/?form=HPFBBK&ssd=2021 0405_0700&mkt=de-CH" /><meta property="og:site_name" content="Bing" /><meta property="og:description" content="This stone bridge, known as Saut de Brot, loo ks li" /><title>Bing</title><link rel="shortcut ic

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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!.!2222222222222222222222222222222222222222222222222222.. ....."..... .....}.....!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\CS6IXJW6\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\CS6IXJW6\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\NewErrorPageTemplate[1]	
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\CS6IXJW6\NewErrorPageTemplate[2]	
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: #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\CS6IXJW6\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:	82388309085BD143E32981FE4C79604DCEFC4222FB2B53A8625852C3572BDE3D3A578DD558478E6A18F7863CC4EC19DFBA3EE78AD8A4CC71917BFFE027DC22 0
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 29.16,14.4 615385 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\CS6IXJW6\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\PA3TC2iNXZkiG2C3IJp5VAvC_yY.gz[1].js	
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\CS6IXJW6\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
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\CS6IXJW6\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:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
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\CS6IXJW6\dnserror[2]	
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:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\dnserror[2]	
Malicious:	false
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\CS6IXJW6\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:	downloaded
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
IE Cache URL:	res://ieframe.dll/down.png
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....#+....I..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\CS6IXJW6\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\CS6IXJW6\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:	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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\favicon-2x[1].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\CS6IXJW6\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:	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:	E7F2603855A16464417B772517676F080CCEFFB8069C687BAC798B7EB2875FCDC207E40E8C56E7CFFD4D56CED572270988599D1D2B73FB8AAA7FDD076FE3E7E 7
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.c lientWidth,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\CS6IXJW6\httpErrorPagesScripts[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):	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
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.su bstring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var pound Index = 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\CS6IXJW6\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, precisi on 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!.!2222222222222222222222222222222222222222222222.. ....."..... .....}.....!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\CS6IXJW6\sjm7ZxOOdUKgLq2Lulikx_Lt20I.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	exported SGML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	4623
Entropy (8bit):	5.164231565021591
Encrypted:	false
SSDEEP:	96:B3D+ca6IQkQQX6hJmK/Vl3A2zLEzvPTkyfXeJLYryYHIZq76/PH:V+ca6IBQQX6aK9l3ASivPTkyWJLh7R
MD5:	8FD5ED5E0730854741D73A66E1C8C124
SHA1:	8A4D348BA92FEBAB3A5FC7FFDED98E0841C3CE9C
SHA-256:	63C3206CB8509C0A2DD25A0AA3555BD49E7B2E24AE95F6CB7E6521D830C986F7
SHA-512:	D52D1CCBBEDDC49B850030E3B2ABA9EADE824AE74EF4FF7055D50EDDCABC7933D6D662FEE8DF0F37B20F096E96908DA0CB89FF8DFC4E6AB14F1255BBDE74 5A40
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/sjm7ZxOOdUKgLq2Lulikx_Lt20I.gz.js
Preview:	define("rmsajax",["require","exports"],function(n,t){function c(){for(var i,n=[],t=0;t<arguments.length;t++)n[t]=arguments[t];if(n.length!=0){if(i=n[n.length-1],n.length==1)ot(i)&&f.push(i);else if(n.length==3){var o=n[0],s=n[1],u=n[2];st(o)&&st(s)&&ot(u)&&(ht(r,o,u),ht(e,s,u))}return window.rms}}function nt(){var i=arguments,n,t;for(o.push(i),n=0;n<i.length;n++)t=i[n],ct(t,r),t.d&&tt.call(null,t);return window.rms}function kt(){var t=arguments,n;for(s.push(t),n=0;n<t.length;n++)ct(t[n],e);return window.rms}function l(){var t,i,n;for(ri(),t=!1,n=0;n<o.length;n++)t=tt.apply(null,p.call(o[n],0))||t;for(i=0;i<s.length;i++)t=ti.apply(null,p.call(s[i],0))||t;if(!t)for(n=0;n<f.length;n++)f[n]()}function tt(){var n=arguments,t,i,f,e;if(n.length===0)return!1;if(t=r[ut(n[0])],n.length>1)for(i=ui.apply(null,n),f=0;f<i.length;f++)e=i[f],e.run=u,dt(e,function(n){return function(){gt(n,i)}}(e));else t.run=u,ft(t,function(){it(t)});return!0}function dt(n,t){var f,u,r;if(!n.state){if(n.state=pt,at(n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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:document,window.navigator.pointerEnabled?u.replace("mouse","pointer"):u,t,!1)}var t="EVT",i=["click","mousedown","mouseup","touchstart","touchend","mousemove","touchmove","scroll","keydown","resize"];n.wireup(t,{load:f,compute:null,unload:e})})(BM)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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):	6861
Entropy (8bit):	7.923522415130838
Encrypted:	false
SSDEEP:	192:pP1/dHNz5HD5uOg6obyVJJ1p+0Z7dxABT0/TWPs:51/9NzFD5uW5VJXp+ggBSCE
MD5:	A9D8276DD966BDF2C3CAA6EC3294B434
SHA1:	6E6CF935ABF2F294CE4DFF4A7817F1A83C6010B8
SHA-256:	D7DCE15491CB66B058EA73EB852CB775C60B1B68D61F4FAD6373556850FB2681
SHA-512:	BB0348419AA17830DEBDA03215A04FA1FBCD96E50D26C4693485A1A6516C56B96C0E2B9EFCE95A58963318C3D36F4CCF04656A1564E3D04BEBCE8F08C139993 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%2fBB1fk7pf.img&ehk=GlhJKmuk54mDmOnKCpgqk3LmCM3IUtj4PpsTmvuZ01s%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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..`r..N....D.pY.....{....wl.+Az.(....B".+..K.x....8...Y...N...K WB.2.`.Z...Y0v0 .{...2..@,~L.....zU.....c..J....?...j..*D.....}.?Z.=.!..{.M.G..>X.....U...5*[....>..J....VW..i@."....^...v!.ORF9.)./l5..[o.At.$q..m.p.F....}....X...s..Uk.q.Z<..q..Ay.....@.Dr.._+.r.bNvw.;.?ZU.^...w....<..u[..\Ae..]Z...Pl..Hx....;U...ZO..Y"..,qkxJH....8....@....- .DM"6....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\th[2].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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\th[2].jpg	
Category:	downloaded
Size (bytes):	6623
Entropy (8bit):	7.943317758283698
Encrypted:	false
SSDEEP:	192:pP7ujoGLjfgUT53aqYOjGRdMjDH3A3iECchM1otj:57ujpLjfgU34dMjDXA3iE3j
MD5:	CBA5738043855BFA16330551C0CB85CE
SHA1:	7774434DCEB28700FFDEF5E08A692D0C1FDD43B0
SHA-256:	7FD41627C564044C5F555B26EDD3F4AA2EC74C5A10DC937B670A7EF0C4020671
SHA-512:	DE2E8ADCB6C64AF7A91EBF3FD2FC44AA52749656C639C68B89D579E5A2F1EE9DC8D039E9D3C060ACD897445A7F80551AD55B0EB184B58AE03CE4C879C88BA ABC
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fjnDt.img&ehk=krsOy%2fAva3slhNFEpo7CxUOQd576Tpz5%2bzpPOtBbEpk%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.....?...d.P.R..}GO.N...yW...)....2....r....90.....o.L.....F.._.j+Q.n.].8.Qn...Z6.z.M=@...k.C..1._.O..Uc0_...\..d.=....a.K.....T.F.;..{Z...hom.F/ K...K..}7.\.{.7...y....e.S.X..}.8...}..dl.a.....0...J...ghA.d...i..K..%zr..6..6.6T.(.[.d.(.Sl...A..mO..m .I...HV. +HV..I.. +I..+HV..m..+E.E<f.3E..d.....la.U..J.E...T..+.....i*.Z...f8.#.....kYIB... ...Ckd...6M..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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):	6671
Entropy (8bit):	7.899478517886581
Encrypted:	false
SSDEEP:	192:pPSbouIRG3An3YTxnqckwkUQLd6kaXwFSg/kb4+:5pG3G3YcskhIkaXwFSmkbP
MD5:	C25DBC173D9815C71AA82862D4F5D156
SHA1:	DD567A753F35636A5B5F941AAA261773BD94397D
SHA-256:	54AE91993F987BE43E3EEEC19D49478573293FA6BA9EBCB639C2262D5C53A2F7
SHA-512:	AFCF82EA614082AA369CAAC0D86F6C6857BE01D2058F96FE4310AE8CC2C0E81D5E698ECABAC6BC3FD5A451628E8C5F5C2C26DE4F23E1CAF6C0F1C47BF1C1 384
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fiU4D.img&ehk=FY0puj0Yi%2bFErHgYnVtZXlknhF5nbFoKkLtnru2aHhU%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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..P....;p..j@.%\....g...?.3F...8.vm../...4C4.ss..#;..r.Q..>.+>.M....C7.....X.]....*.....]7..#%.2....O.<.d.t.2I4n.<.X.Y....1.(.i.+3(..Y.9...."..ca.....r.....TL..w..:.|.....<Q.....>i.h..7...P../.....hGU...t...F\...:....s.95.Fu..".1...a..v?l.%..$..;.+jkI.=z7W!..px8.....|.6Gs..0U...<.=Y$C..'..U.1....f.../Pq..q..r.....e.v.s.....a.(..1.....q..._

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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:	DCA2E67C46CFF1B9BE39CE8B0D83C34173E6B77EC08FA4EB4BA18A4555144523C570D785549FED7A9909C2E2C3B48D705B6E332832CA4D5DE424B5F7C3CD5 BE
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\OR0WKIO1\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\GiGr-rA9TBhE2c3LJn7PvDweiOo.gz[1].js	
Entropy (8bit):	5.158592433297743
Encrypted:	false
SSDEEP:	6144:1irrzbB3LH7gaV6Z8LAfP0Rp6Izc04YFdNwRm2EjXi4SG7oIBYQmzeH:aHNfi4KwYQmzeH
MD5:	F279A46B56038C41BB3FC11D67D0FE46
SHA1:	B48121E695FD6483CAA7F48DE73FE9F121777109
SHA-256:	A9EA274B393E34591387AC0B4DE594BEE296386543DE34F4897281324DB0DCBB
SHA-512:	4C1754CF5E368D8CE86B135B789A4FF4BAAD1419F30A1EB3B65EAB62217C054D0066EA5FC22B5AA7643EA959854EBC2029B39CB7D1AEAAFB78B95A2A46430F84
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.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\OR0WKIO1\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
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\OR0WKIO1\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
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\OR0WKIO1\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\NGDGShwgz5vCvyjNFyZiaPlHGCE.gz[1].js	
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\OR0WKIO1\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:+FE64YTsQF61KWllWeM2lSoiLKiUfpIYdk+fzvOMuHMH34tDO8XgGQE3BUf4JPwk:+FdF6UYXEBi9kIHIB1UY
MD5:	EF3DA257078C6DD8C4825032B4375869
SHA1:	35FE0961C2CAF7666A38F2D1DE2B4B5EC75310A1
SHA-256:	D94AC1E4ADA7A269E194A8F8F275C18A5331FE39C2857DCED3830872FFAE7B15
SHA-512:	DBA7D04CDF199E68F04C2FECFDADE32C2E9EC20B4596097285188D96C0E87F40E3875F65F6B1FF5B567DCB7A27C3E9E8288A97EC881E00608E8C6798B24EF3 F
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.w lImgLg?{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.he aderLoginMode=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.popu pLoginUrls)&&(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.p op=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\OR0WKIO1\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; (m ainWindow = 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\OR0WKIO1\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\UYtUYDcn1oZlFG-YfBPz59zejYI[1].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\OR0WKIO1\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=9002
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\OR0WKIO1\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....#+....I..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\OR0WKIO1\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\OR0WKIO1\k5oM71-Oyo7w7ptkcB_2S5dIr7I.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	21824
Entropy (8bit):	5.243380331742482
Encrypted:	false
SSDEEP:	384:HXpeDC+2uguwBYFsOZrSzz3wp0OxAmzjEHU:HXpeDz2gFsOZrOXWz4HU
MD5:	071CABC528DA3CDD5BD5C7F0EC48ED96
SHA1:	8B665A2DA630D6711E01E838877510F48C40E9CE
SHA-256:	9871F6289648EEA5CB484C2307C4E7BCDF3857AEB27EB07E0ACFD4C1B77EDBB5
SHA-512:	771DA4D3B22B53C5B1B1D2DF1B923B78124A7F92576700F7E988A1E40C2806CB2366D52C556F1FD49862B1A584D871ED7207B54174172740B4ED125AAD4C531F
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/k5oM71-Oyo7w7ptkcB_2S5dIr7I.gz.js
Preview:	(function () {.. if (typeof window !== 'undefined') {.. (function (arr) { arr.forEach(function (item) { if (item.hasOwnProperty('remove')) { return; } Object.defineProper ty(item, 'remove', { configurable: true, enumerable: true, writable: true, value: function remove() { if (this.parentNode === null) { return; } this.parentNode.removeChild(this); } }); }); })([Element.prototype, CharacterData.prototype, DocumentType.prototype]);.... !function(e,n){"object"==typeof exports&&"undefined"!=typeof module?n():"fun ction"==typeof define&&define.amd?define(n):n()}(0,function(){"use strict";function e(e){var n=this.constructor;return this.then(function(t){return n.resolve(e()).then(function() {return t})},function(t){return n.resolve(e()).then(function(){return n.reject(t)})})}function n(e){return!(!e||"undefined"==typeof e.length)}function t(){}function o(e){if(!(this in stanceof o))throw new TypeError("Promises must be constructed via new");if("function"!=typeof e)throw new Type

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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:	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/lK_FmcR4naKX9hplwfe9ify1hf4.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\OR0WKIO1\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:	downloaded
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:	4F0078431E86CCD8C0B3DE7E4F7CC10B184DC5376AD10C224EC081DAE1B9D16509E01A95CE3F3B4F7C394EC2C52782E4CB9AC2DE8C12CA0FFC9CC66C01C5 AFD
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/sTWC0LplwPyIP_jw8VjHps800ZQ.gz.js
Preview:	var customEvents,__spreadArrays,fallbackReplay,EventLoggingModule;_w.EventsToDuplicate=[];_w.useSharedLocalStorage=!1;define("shared",["require","exports"],func tion(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}functi on 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.fromElemen t: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\OR0WKIO1\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\swyt_VnIjJDWZW5KEq7a8l_1AEw.gz[1].js	
Category:	downloaded
Size (bytes):	2298
Entropy (8bit):	5.34865319631632
Encrypted:	false
SSDEEP:	48:KWEkTScZVcMBOwXhzwBi88RnX8ec0T39B8onA008xG9FLCx3w0S5xJ:KWEkTDZVXpR0BiXjTtB8mA0zxWsx3PG/
MD5:	A8D7D1B3681590980B2D7480906078DB
SHA1:	C9A7A400DB1EBAD4DCA028546EE5F5B2EF4136BD
SHA-256:	1390485DC88B6230389D9C95232A3710BF38D47271708A279B12D7E68E43F649
SHA-512:	710D31EFD76614EC4C94888E2FCC49ABAB50EF406FC0F1C5C10D8AA21D4E9F349DE78068B2BAFE495C074AB4E6EC0A5D44EB5506B2D79C78707A23C1D8206664
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.textContent!==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\OR0WKIO1\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):	317464
Entropy (8bit):	7.978513703412309
Encrypted:	false
SSDEEP:	6144:LpczWY+0f/R9tTGg5oOxoaDdSjmrPtX82LdFzDLBCmfWAR:lczNJTX5oO6UdEmrZhLjhCmfWw
MD5:	6F4EBEE6F946368A02FCF8615CFF289A
SHA1:	FDB7A1DBFE702E4ACB2CE3859E6CD1627E908B47
SHA-256:	574BC892E7F45D4CD74153511B183DB04680551E80EB389ECD619950081852B2
SHA-512:	A37BE5349A4A802E46300CE7C4AF3A8D154BA7ED06C94F4DBE372920ACE25237E954094EEF60D3EF8C350F65761FD0A224A22A23AE31C7405F67896C1EDD3DB6
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?id=OHR.SautduBrot_ROW9659507110_1920x1080.jpg&rf=LaDigue_1920x1080.jpg
Preview:	......JFIF.....C.....$..$-"."-)#""#)8/////8A;;;;;;AAAAAAAAAAAAAAAAAAAAAAAAAAAA...C.....#..#1#.#1?1&&1?A?;/;?AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.....8...".....E.....!..1AQ."aq2...B.....#R.b.3r...$C..S...%4cs.....5.....!1.AQ."a2q....B...Rb....#3r.....?..".s.2f... ....!.=n...v..i.X...1..x.....v.['.?...b.f...Y.r....j....?.x.G.&..}..;....$}~.ki..bx.GsGr.y..iF.$..5uk.....>.?..T.~..Z5.. .....z..C.$.j.}.$A.....z..R..A....L....)f.&.....d...:...k...3\.....m..$...m.+.A.....v..3..J..n.L.....Ze.m.[..V....u.a+:..$.....6.....7`w.)%.4.4..i.....{.A9..P+....Z.$.|w...g..I-%q.w.%..+v....=.Wql.....hLr..c ..zP].I..p._jU...>.j.6...6..u...k<S...T.wy...x>..[A.o...;.V.....%R.....>!R.....i..O.....\O...>....."Cz..7n..).....>b..8.t..[h..:{M..u.%..&K/u..).Qk.....X..k..s..M9]/r.....*L.....9.....A.=P.J5.....CN...Fm.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\th[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	55153
Entropy (8bit):	7.988984887631975
Encrypted:	false
SSDEEP:	1536:OCOPysX7Wz+FFHY8OXIkXN4/aESRIpKK8NLz+S45T:pO9X79FF48O5qSRGKKr
MD5:	C30CEE8C669B32845A7C1D9925C6AD12
SHA1:	35590990C7D5345C9C34852692A93C409686A375
SHA-256:	4F2E3C88208BC3BA6A68F21F0AC7CAFB5E886C7EB3D7A4A86DEF72D8E590B62F
SHA-512:	F3E5B5FD430D8EBCA17032493A7BAB4792E6B22193B7104A34572B89500FF95A8B46615EC27022C55AABC1B5256E683D1701089556A1C927A3A14430E3524210
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fks8r.img&ehk=MqQZgZrj4DCNtpVl11d0lE988SsVQ%2fcHQ6mTM6D%2fYss%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	.PNG.....IHDR.....<.q.....sRGB.....gAMA.....a.....pHYs.....#.u....IDATx^..g..I.-.....aGddFvgv.....Y....&8. "..s.9'..9.s. \.o.9.7.dV..@..z.....jj..TU...*..Z..O..}....c....m..ul.....?>.....u...c...v....>.....?s.....?S.*.O..a....c?.....xw.....1.}U><..`.....8.^..66..a.~.....\.....:..v..w.]..w.?x.....u..B..?....._P....[.....s]..y..\..yY.8"^=.....=..^.}z.....7.....>8.....x...>{4n..z...7.....<.....]..k>.. j.>....\...`.}.....?.l};.}.....r..z...O.....<...k..8.....g.>..;.u.]W...p....~.....^.1.....o....~.s.1(<..[.....Y]].....>.=.k.*.yU/W....pJ..^=...s....=...[.Z.c...._...'...>..}..X....]...w.V.....C..k.....\.....k..=..C....-yU.....r$.....Y.. .....p.y.....x.L.;9.=>.=....t..7c.....q.....`....p...Z.?....w.S_.v...p...{.3..7oD....).o.....8..u..+..{..s.9:R=9.....R~..#...sY_sdg.....odi.....uV.y.S.....w.....9..D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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):	5551

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\th[2].jpg	
Entropy (8bit):	7.912556663981365
Encrypted:	false
SSDEEP:	96:5PEeA7XysnXLdoR1eOZzFjcBy6nSo/Jy8LM4FVlH2OGLk:5PpA7pnbdoFfW73/kX4FVl2Y
MD5:	F3A2F80F58F49597FF4E785E532006B1
SHA1:	85DCB4EB6C5EBF9DC9074876802754A8A441FC85
SHA-256:	10252B2E9BBED9FA101E73283D7E05FC07843CB416701FF80A8B157B81A95E7F
SHA-512:	4D0ADC467E3DBDE9B1503B3BD6FF88C19055AD4323F2A641AB5653BB6014EBD35C6796D2E4FC12F4EF88F8D42DC608C70B42495A810E4D60596C91F3737602B
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkpJk.img&ehk=HiIriPbRsbFHpW1R13YXE4bkulV96V5SFczX3iTffRg%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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..@)qN.....&).b...F.~(.0#.F.~(..3.....".0#9....J.Bd..8...._rk...#..[.....<..k.II.....k.wP....9.U.....x...`7...YI..R...^k.;...,$-.C....o%..6....k....zt..z.q.....E.gz.V..".R1..(RKa5r;k.4 -..#....~ .1Gmo..H..5L...s\r....4...=.G;..Dv...?z0=|.SK...-./....b.8..\JI..N;T...9..{F?f.....s...+..~Q.y.....G...jO.q.Z.jV.....W*%.....z.9_#$W.(X.E..g.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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):	4602
Entropy (8bit):	7.919085409507157
Encrypted:	false
SSDEEP:	96:pPEQIac5U07wxonYM7ZCOPHZ3V4DItC+Es/YzbvLSLIBpxrDn5M:pPjeyynnlCoZ32In4TL6CHD+
MD5:	8816AF91855EFB0BB97FAF7429A17E5A
SHA1:	7FFA5A24554D8CA448E6D1F98A7AC31F36CB2FC7
SHA-256:	1C54DB3F6FA0501AB0C6ACC1BFFC8629009F76BE5AA6DE4239FEB24E3C6AEBFC
SHA-512:	F615D37B9E117B9E1A8DC287DC4FD5888BE85F8CB9E9C66E49B547A0D3969611771660322511 7D05D7E30734131D15A5C651EFD0B6E9DA546825352B25CCF082
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\OR0WKIO1\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):	3561
Entropy (8bit):	7.878440257298762
Encrypted:	false
SSDEEP:	96:pPEEPBM3vBIZmcrx2rYixTrLuYrBNnZ+E1Ahod:pPRBM3ZTfTr35+hhod
MD5:	3320821DDAAD044CFC063CC415815224
SHA1:	547FA2595126A16D9DC3027A90E9E1C8EEF6CCA5
SHA-256:	021962EB9AA429F9CFA108D467E93503D2247BDD3CD414371FD8DCB304860468
SHA-512:	6BBC41216196099A273E4B0E99B696F6D60B8ABF816C828901A678E758B9531A9E3C3D6110BAE4C850A66EDBCE34952F410FFFBB4FBF745B505C8547F71842A4
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1f7Ufv.img&ehk=1wok0OMghjUfFYwP20DoV2Cjfml%2bU7Yr2y7aWYwLa%2fE%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.....?..(.....4..(...(...(...(....J.X.J.m?1.`..).E.....,+.....=.?.....TC.|...S.!'..F....."(.7A.5.X.K67.('q..)..*.. .\.*(.5Hx...'..\i.["\.f..^-B.o.2...C.....qkq.'.QKJ)..S.&s.).BX...X.|.*{..` .....i.K.....[..f..Q.?OZ...T.o w....eP.....@.{.a.....*.j.[.9....T....d....G....._JO%}*d.G Se.a..v..+..._E@.._.....&.....'u..OE.3...c...{..!.N...#..Ue-.nmA.e.%.I..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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):	4856
Entropy (8bit):	7.9123534754158555

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\th[5].jpg	
Encrypted:	false
SSDEEP:	96:5PEVumHHUZt9z9DcmTUovcPyREwSkNYYyj3XgquvGr4j:5PKVHqt9z9l7PyuaY1jHBuJ
MD5:	FFB90C8503E1B6E7DDFF9B0D34F8224A
SHA1:	B5C33E88BE9BF2BDFAF1413BBB3DB4AAC7AD54E5
SHA-256:	4C7D8830EF2A36840DA850A7203BFB300E2D62282DBCBE4950BE750699C61E24
SHA-512:	D959DF12C4EF4CD777AB6828ED9CE346CB6DC04FAA40E6294D1764F5190D655B491E33B3AFAD5792807A5815EA647B0D787D3B4D3A755D4A7FAECA21F18E2FBA
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fk9Yx.img&ehk=ZhorGYcGsv4ONnFmqu1DK3dvGXtaoQL2kkyRlkNkono%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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..v....2...pA..<.T..pz<+u..D.*e...s.+...z...zT.....3.9#.r.....O.pFqG...'...M.N$..1..a....I5.....\!.iI.m. v.*,>k.%.,8C..X...8>.V.[.kG.Xn\....6e.P.#.._....{..-.rT....."eQ-.....f;c.YcV._&..~.\.#i.Q...d....+_...q.e..2B....hW.2c.8=*9".....G...9..'...t..T..wn.Bh'.-..T.q.]j..C.Fb.H.F..g.....Y.~..r:}}*..r6...2*.....&.n...%....%.....-fI..].du.w.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\th[6].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 640x640, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	6676
Entropy (8bit):	7.934622305650732
Encrypted:	false
SSDEEP:	192:5Pwl4vzYTH57OnRURC0JJGkmMJlcIi7r3E:JHyH5YRMJbJl1in3E
MD5:	C877FCFEE45C9F07ED11C2BCEDF9A443
SHA1:	D2C6249174697B5D7C2DAB1CD4508AFFFC54EB69
SHA-256:	FB74581CCDB447D45F1B057F8D7FB4ED86FB2A942290C6B6E8EE55CD5EAE802C
SHA-512:	75BF96F9C708F2F2311867BBC1657DA82D2BB7F8A9C48E03CD3E61F062E7B3B1E3D32D37735117BF65B9ACC08C4AD6E9808EB8A0F6F7197C57B2BBBF2CBA11C6
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fk5r2.img&ehk=NrXMj7MDjTlxvuYX78PszW7orgLDcMKaJhC4fXgM1dg%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.....?...d..jlu.....8.1...^.{.A..5..Bh...=.N..|.....].O^[.k.prwG]..l.01.NA..k.....|.=.?.zo.": .4...q..|%.`....?.Y.)..f'.4l.8m.C..l .....;..=...t9.;...'."z'..-..._..0..O1...n..!S..~..z..".\m6.....-..?.....{.a..r..3.Rm9..n.....-.....h.#.6.z....=.....eH.....py..~..za.....L...SF..%.....=...G..O=s..J.:.u.K...SE....:.?.H|+.s.....=...D.h..pI..Q.I=x....h

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\uYzy_SF_Qx-quOm8IecsaqSoOd0[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1400
Entropy (8bit):	4.810462023135915
Encrypted:	false
SSDEEP:	24:t4LxHXU4dxCey0fA53J/S/7/sG5BmefEqrR5GTGOby2NF2E/:+x3U4S55Z/aB5BmefEqrRYK6
MD5:	2C4837A751CDB1A7366A56A0BD33EF59
SHA1:	B98CF2FD217F431FAAB8E9BC21E72C6AA4A839DD
SHA-256:	AA593C656009A40AC1782DD6FEE1EF31F9D4CCAD9F3F657DDF9A72C1EB7E553A
SHA-512:	79DBB36F29034FCB52BA9C51A01346F9CEA694CAEBA9B149EEB66DB732B73C01C71FB7F4FBA892E67523E955153FAE4D0148C1024291CBBA0CBFC26FC5C8641E
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/uYzy_SF_Qx-quOm8IecsaqSoOd0.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" viewBox="0 0 40 40" style="width:64px;height:64px;">.. <style type="text/css">.. .anim {.. animation-name: blink;.. animation-duration: 1s;.. animation-iteration-count: infinite;.. fill: #05E9F5;.. transition-timing-function: linear;.. }.. @keyframes blink {.. 0% {.. opacity: 0.. }.. 50% {.. opacity: 1.. }.. 75% {.. opacity: 1.. }.. 100% {.. opacity: 1.. }.. }.. .delay1 {.. animation-delay: 0s;.. }.. .delay2 {.. animation-delay: .125s;.. }.. .delay3 {.. animation-delay: .25s;.. }.. .delay4 {.. animation-delay: .375s;.. }.. .delay5 {.. animation-delay: .5s;.. }.. .delay6 {.. animation-delay: .675s;.. }.. .delay7 {.. animation-delay: .75s;.. }.. .delay8 {.. animation-delay: .875s;.. }.. </style>.. <circle class="delay1 anim" cx="20" cy="8" r="3" />.. <circle class="dela

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.34393990581221
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:	KcFVz0y2si.dll
File size:	120716
MD5:	a1e2a0759924852c160b109f73ffd091
SHA1:	7ebf1673c6661cfddfa4891c6e455111ce331333
SHA256:	657455d2129ca06ee85cb534186d7d80b648e10f7f9e50f43cc5f56fbc7d154c
SHA512:	b11faf5946d3f5f83d87be899ceb10f15501dccf80d88e51c3227b25331c6737e276665c2992c6eefa2074f5140d1262a0a68ede61ac8cec810f6d737c179e84
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
push esi
mov dword ptr [esp], FFFF0000h
call 00007F3CECA801E0h
push ecx
add dword ptr [esp], 00000247h

Instruction
sub dword ptr [esp], ecx
push ecx
mov dword ptr [esp], 00005267h
call 00007F3CECA7CB89h
push esi
mov esi, eax
or esi, eax
mov eax, esi
pop esi
jne 00007F3CECA81C82h
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 00007F3CECA81C5Eh
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

Name	Virtual Address	Virtual Size	Is in Section
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

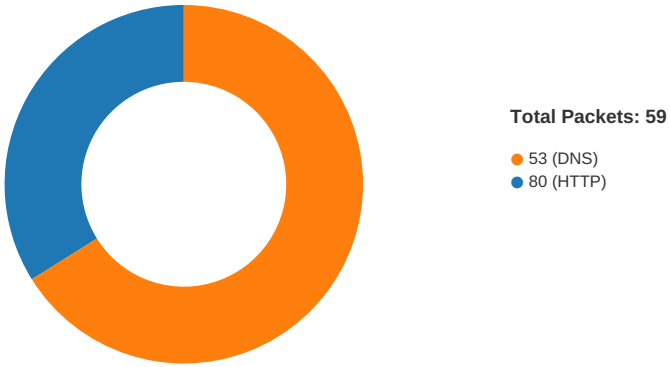
DLL	Import
user32.dll	GetActiveWindow, CheckDlgButton, CheckMenuItem, CheckRadioButton, CheckMenuRadioItem
kernel32.dll	GetProcAddress, LoadLibraryA, VirtualProtect, VirtualAlloc, lstrlenA, GetCurrentThreadId, GetCurrentProcess, GetCurrentThread, Module32FirstW
ole32.dll	OleInitialize
comctl32.dll	DPA_Sort

Exports

Name	Ordinal	Address
StartService	1	0x1000b959

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 5, 2021 22:38:08.764158010 CEST	49739	80	192.168.2.4	185.243.114.196
Apr 5, 2021 22:38:08.764426947 CEST	49740	80	192.168.2.4	185.243.114.196
Apr 5, 2021 22:38:09.772320986 CEST	49740	80	192.168.2.4	185.243.114.196
Apr 5, 2021 22:38:09.772366047 CEST	49739	80	192.168.2.4	185.243.114.196
Apr 5, 2021 22:38:11.788331985 CEST	49740	80	192.168.2.4	185.243.114.196
Apr 5, 2021 22:38:11.788552999 CEST	49739	80	192.168.2.4	185.243.114.196
Apr 5, 2021 22:38:15.806183100 CEST	49742	80	192.168.2.4	185.243.114.196
Apr 5, 2021 22:38:15.806195021 CEST	49741	80	192.168.2.4	185.243.114.196
Apr 5, 2021 22:38:16.804202080 CEST	49741	80	192.168.2.4	185.243.114.196
Apr 5, 2021 22:38:16.819881916 CEST	49742	80	192.168.2.4	185.243.114.196
Apr 5, 2021 22:38:18.804348946 CEST	49741	80	192.168.2.4	185.243.114.196
Apr 5, 2021 22:38:18.851183891 CEST	49742	80	192.168.2.4	185.243.114.196
Apr 5, 2021 22:38:32.121098042 CEST	49743	80	192.168.2.4	185.243.114.196
Apr 5, 2021 22:38:32.121400118 CEST	49744	80	192.168.2.4	185.243.114.196
Apr 5, 2021 22:38:33.133723974 CEST	49744	80	192.168.2.4	185.243.114.196
Apr 5, 2021 22:38:33.136876106 CEST	49743	80	192.168.2.4	185.243.114.196
Apr 5, 2021 22:38:35.149408102 CEST	49744	80	192.168.2.4	185.243.114.196
Apr 5, 2021 22:38:35.153387070 CEST	49743	80	192.168.2.4	185.243.114.196
Apr 5, 2021 22:38:39.170775890 CEST	49745	80	192.168.2.4	185.243.114.196
Apr 5, 2021 22:38:40.165452003 CEST	49745	80	192.168.2.4	185.243.114.196

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 5, 2021 22:36:28.548943043 CEST	59042	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:36:28.597814083 CEST	53	59042	8.8.8.8	192.168.2.4
Apr 5, 2021 22:36:29.724076986 CEST	56483	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:36:29.778336048 CEST	53	56483	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:03.830044031 CEST	51025	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:03.884473085 CEST	53	51025	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:08.102475882 CEST	61516	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:08.148294926 CEST	53	61516	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:09.622541904 CEST	49182	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:09.671269894 CEST	53	49182	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:12.517050028 CEST	59920	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:12.562946081 CEST	53	59920	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:14.172424078 CEST	57458	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:14.218343973 CEST	53	57458	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:15.337971926 CEST	50579	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:15.383836031 CEST	53	50579	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:17.715152025 CEST	51703	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:17.761555910 CEST	53	51703	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:18.481370926 CEST	65248	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:18.527244091 CEST	53	65248	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:19.719419003 CEST	53723	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:19.778256893 CEST	53	53723	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:20.940169096 CEST	64646	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:20.997154951 CEST	53	64646	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:22.987382889 CEST	65298	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:23.033243895 CEST	53	65298	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:23.326570034 CEST	59123	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:23.384947062 CEST	53	59123	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:24.412733078 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:24.438082933 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:24.469476938 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:24.485538006 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:24.769974947 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:24.815906048 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:25.057317019 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:25.122906923 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:25.761248112 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:25.824556112 CEST	53	49257	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 5, 2021 22:37:25.834578991 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:25.888695955 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:26.462814093 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:26.517333984 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:27.283225060 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:27.329174042 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:28.127063036 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:28.186378956 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:29.885588884 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:29.932261944 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:30.670151949 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:30.720211029 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:53.291074038 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:53.348527908 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:54.302594900 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:54.359628916 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:55.320905924 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:55.382958889 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 5, 2021 22:37:57.334558964 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:37:57.383399963 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 5, 2021 22:38:01.334794998 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:38:01.383512974 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 5, 2021 22:38:07.635390997 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:38:07.691448927 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 5, 2021 22:38:08.662898064 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:38:08.744667053 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 5, 2021 22:38:09.429306030 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:38:09.540498972 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 5, 2021 22:38:09.544836044 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:38:09.602593899 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 5, 2021 22:38:09.608922958 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:38:09.666426897 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 5, 2021 22:38:22.879291058 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:38:22.933897018 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 5, 2021 22:38:31.118469954 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:38:31.174829006 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 5, 2021 22:38:32.032649994 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:38:32.102869034 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 5, 2021 22:38:39.172539949 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 5, 2021 22:38:39.226543903 CEST	53	61721	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 5, 2021 22:37:25.761248112 CEST	192.168.2.4	8.8.8.8	0x86fc	Standard query (0)	login.micr osoftonline.com	A (IP address)	IN (0x0001)
Apr 5, 2021 22:38:08.662898064 CEST	192.168.2.4	8.8.8.8	0x1e3f	Standard query (0)	under17.com	A (IP address)	IN (0x0001)
Apr 5, 2021 22:38:22.879291058 CEST	192.168.2.4	8.8.8.8	0xd986	Standard query (0)	under17.com	A (IP address)	IN (0x0001)
Apr 5, 2021 22:38:32.032649994 CEST	192.168.2.4	8.8.8.8	0x5e2b	Standard query (0)	under17.com	A (IP address)	IN (0x0001)
Apr 5, 2021 22:38:39.172539949 CEST	192.168.2.4	8.8.8.8	0xbea6	Standard query (0)	under17.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 5, 2021 22:37:25.824556112 CEST	8.8.8.8	192.168.2.4	0x86fc	No error (0)	login.micr osoftonline.com	a.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Apr 5, 2021 22:37:25.824556112 CEST	8.8.8.8	192.168.2.4	0x86fc	No error (0)	a.privatel ink.msiden tity.com	prda.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Apr 5, 2021 22:37:25.824556112 CEST	8.8.8.8	192.168.2.4	0x86fc	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 5, 2021 22:37:25.888695955 CEST	8.8.8.8	192.168.2.4	0xa1cf	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 5, 2021 22:38:08.744667053 CEST	8.8.8.8	192.168.2.4	0x1e3f	No error (0)	under17.com		185.243.114.196	A (IP address)	IN (0x0001)
Apr 5, 2021 22:38:22.933897018 CEST	8.8.8.8	192.168.2.4	0xd986	Server failure (2)	under17.com	none	none	A (IP address)	IN (0x0001)
Apr 5, 2021 22:38:32.102869034 CEST	8.8.8.8	192.168.2.4	0x5e2b	No error (0)	under17.com		185.243.114.196	A (IP address)	IN (0x0001)
Apr 5, 2021 22:38:39.226543903 CEST	8.8.8.8	192.168.2.4	0xbea6	Server failure (2)	under17.com	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 4200 Parent PID: 5932

General

Start time:	22:36:35
Start date:	05/04/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\KcFVz0y2si.dll'
Imagebase:	0xd80000
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: 00000000.00000003.798289692.0000000003ACB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.798356915.0000000003ACB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.912950369.0000000001180000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.798241587.0000000003ACB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.798380410.0000000003ACB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.798275065.0000000003ACB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.798260213.0000000003ACB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.877675545.00000000039CD000.00000004.00000040.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: 2936 Parent PID: 4200

General

Start time:	22:36:35
Start date:	05/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\KcFVz0y2si.dll',#1
Imagebase:	0x11d0000
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: 1852 Parent PID: 4200

General

Start time:	22:36:36
Start date:	05/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\KcFVz0y2si.dll,StartService
Imagebase:	0x1320000
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: 00000002.00000002.678640834.00000000011D0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 408 Parent PID: 2936

General

Start time:	22:36:36
Start date:	05/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\KcFVz0y2si.dll',#1
Imagebase:	0x1320000
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: 00000003.00000003.800812479.0000000004D38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.800782996.0000000004D38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.800751690.0000000004D38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.912982119.00000000001D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.800877488.0000000004D38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.800857311.0000000004D38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.800835964.0000000004D38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.800898920.0000000004D38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.800911923.0000000004D38000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 5740 Parent PID: 800

General

Start time:	22:37:21

Start date:	05/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7d3ff0000
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: 1260 Parent PID: 5740

General

Start time:	22:37:22
Start date:	05/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5740 CREDAT:17410 /prefetch:2
Imagebase:	0xf10000
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: 2212 Parent PID: 800

General

Start time:	22:38:06
Start date:	05/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7d3ff0000
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: 4592 Parent PID: 2212

General

Start time:	22:38:06
Start date:	05/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2212 CREDAT:17410 /prefetch:2
Imagebase:	0xf10000
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: 5348 Parent PID: 2212

General

Start time:	22:38:07
Start date:	05/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2212 CREDAT:17414 /prefetch:2
Imagebase:	0xf10000
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: 1076 Parent PID: 800

General

Start time:	22:38:29
Start date:	05/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7d3ff0000
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: 2440 Parent PID: 1076

General

Start time:	22:38:30
Start date:	05/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1076 CREDAT:17410 /prefetch:2
Imagebase:	0xf10000
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

Disassembly

Code Analysis