ID: 382127
Sample Name: bTjvWUTLid.dll
Cookbook: default.jbs
Time: 21:26:31
Date: 05/04/2021
Version: 31.0.0 Emerald

Table of Contents

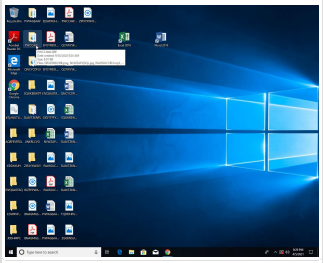
Analysis Report bTjvWUTLid.dll

Overview

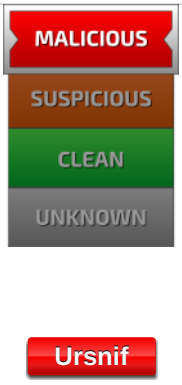
General Information

Sample Name:	bTjvWUTLid.dll
Analysis ID:	382127
MD5:	9064c426999ab9..
SHA1:	cc20039678658d..
SHA256:	7d80947ba67843..
Tags:	dll Gozi ISFB Ursnif
Infos:	

Most interesting Screenshot:



Detection



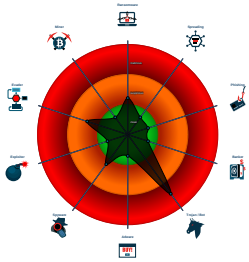
Ursnif

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 process in suspended mo…
- Detected potential crypto function

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 4740 cmdline: loaddll32.exe 'C:\Users\user\Desktop\bTjvWUTLid.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 5936 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\bTjvWUTLid.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 4700 cmdline: rundll32.exe 'C:\Users\user\Desktop\bTjvWUTLid.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6076 cmdline: rundll32.exe C:\Users\user\Desktop\bTjvWUTLid.dll,StartService MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 2296 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6212 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2296 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 6356 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6380 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6356 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 1328 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6356 CREDAT:82952 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 6652 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5024 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6652 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6584 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6652 CREDAT:17414 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
[
  [
    {
      "RSA Public Key":
"Om1HeBhXBR6NHvmWFGSB2kyl5mdcRMsb8ux2uo9VgGW0O2LzHZKk3w9bxw9stgphU0ayytcOYkK6GCNJlKSeMTZJ5WPgZiX+MaXiUccStEUTXkW1ubp0gdr16sb5U4M+rzWWPvc3s7bj9o1yqSJtP7PmMVp7E+3llLULQ9/DZbAD7SXa
ft6wcY8wFj5kI+8D"
    },
    {
      "c2_domain": [
        "bing.com",
        "update4.microsoft.com",
        "under17.com",
        "urs-world.com"
      ],
      "botnet": "5566",
      "server": "12",
      "serpent_key": "10301029JSJUYDWG",
      "sleep_time": "10",
      "SetWaitableTimer_value": "0",
      "DGA_count": "10"
    }
  ]
]
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000003.294061363.0000000005418000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.322688241.0000000003C4B000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000002.468904575.0000000003A4F000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.293962458.0000000005418000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.322716434.0000000003C4B000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 17 entries				

Unpacked PEs

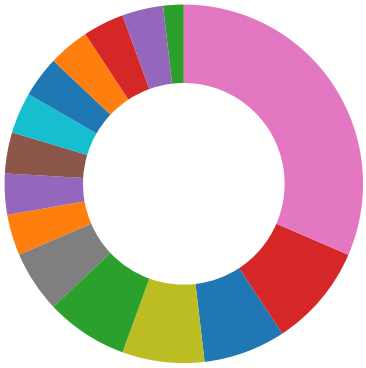
Source	Rule	Description	Author	Strings
4.2.rundll32.exe.10000000.5.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
4.2.rundll32.exe.30b0000.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.2.rundll32.exe.2b20000.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.2.loaddll32.exe.fe0000.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.2.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

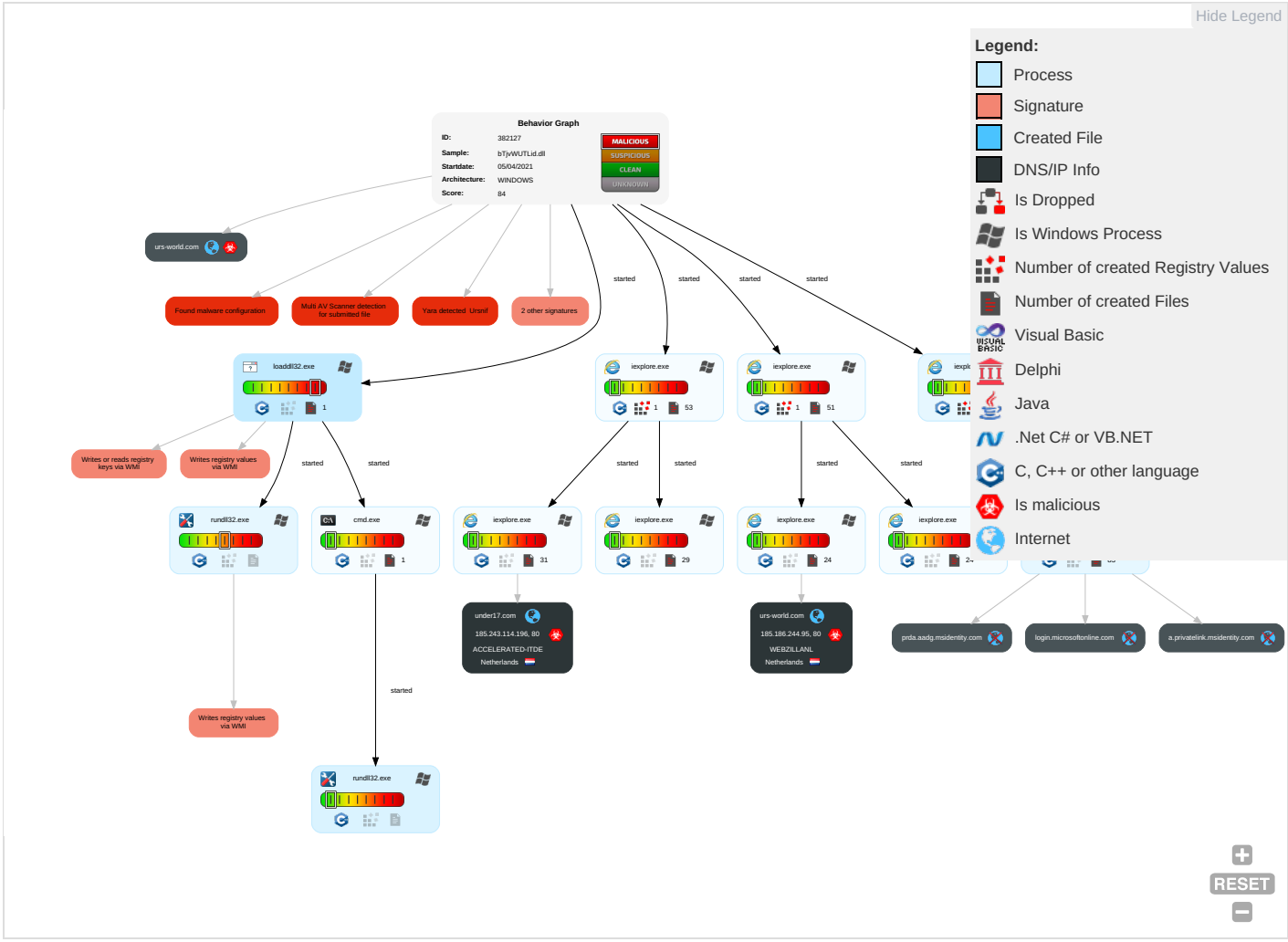
Remote Access Functionality:

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

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
bTjvWUTLid.dll	51%	Virustotal		Browse
bTjvWUTLid.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.47f0000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
4.2.rundll32.exe.10000000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
1.2.loaddll32.exe.30b0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
1.2.loaddll32.exe.3090000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
1.2.loaddll32.exe.10000000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://under17.com	0%	Avira URL Cloud	safe	
http://under17.com/joomla/G2ZDC8nn3wolJdH4SM/R_2FZIZic/jRRSf9Lfj1TfaLV_2FrF/Xa4iMZXZ_2FvgVSu1Or/GmOK	0%	Avira URL Cloud	safe	

Domains and IPs

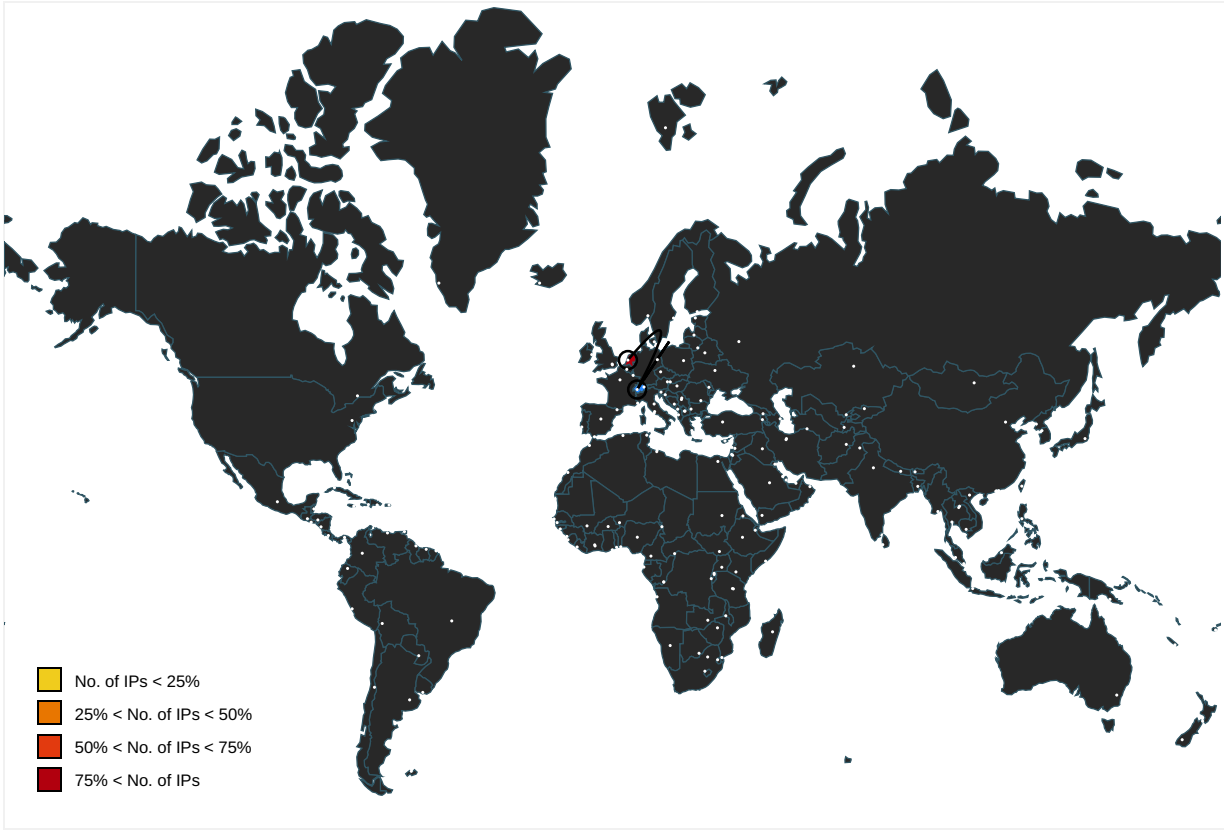
Contacted Domains

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://login.microsoftonline.com/common/oauth2/authorize?client_id=9ea1ad79-fdb6-4f9a-8bc3-2b70f96e	{7FB5F6EF-9690-11EB-90E4-ECF4BB862DED}.dat.12.dr	false		high
http://feross.org	GiGr-rA9TBhE2c3LJn7PvDweiOo.gz[1].js.13.dr	false		high
http://under17.com	rundll32.exe, 00000004.00000002.468417871.00000000030DA000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://under17.com/joomla/G2ZDC8nn3wolJdH4SM/R_2FZIZic/jRRSf9Lfj1TfaLV_2FrF/Xa4iMZXZ_2FvgVSu1Or/GmOK	~DF058AFC2113F0053A.TMP.24.dr, {9BF67421-9690-11EB-90E4-ECF4BB862DED}.dat.24.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	382127
Start date:	05.04.2021
Start time:	21:26:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	bTjvWUTLid.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:	36
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@20/69@9/2
EGA Information:	Failed

HDC Information:	• Successful, ratio: 53% (good quality ratio 50.9%) • Quality average: 80.1% • Quality standard deviation: 27.8%
HCA Information:	• Successful, ratio: 86% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 92.122.145.220, 168.61.161.212, 20.82.210.154, 184.30.24.56, 88.221.62.148, 13.107.21.200, 204.79.197.200, 40.126.31.143, 40.126.31.135, 20.190.159.138, 20.190.159.134, 20.190.159.136, 40.126.31.6, 40.126.31.4, 40.126.31.141, 20.190.160.74, 20.190.160.3, 20.190.160.7, 20.190.160.135, 20.190.160.130, 20.190.160.131, 20.190.160.68, 20.190.160.133, 92.122.213.247, 92.122.213.194, 51.103.5.186, 8.241.79.126, 8.238.27.126, 8.238.85.126, 8.238.35.254, 67.26.137.254, 152.199.19.161, 20.54.26.129, 20.82.209.183 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, store-images.s-microsoft.com-c.edgekey.net, bing.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, go.microsoft.com, login.live.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, www2.bing.com, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ie9comview.vo.msecnd.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, login.msa.msidentity.com, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, dub2.current.a.prd.aadg.trafficmanager.net, store-images.s-microsoft.com, www2-bing-com.dual-a-0001.a-msedge.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.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

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.243.114.196	KAsJ2r4XYY.dll	Get hash	malicious	Browse	
	swlsGbeQwT.dll	Get hash	malicious	Browse	
	document-1048628209.xls	Get hash	malicious	Browse	
	document-1771131239.xls	Get hash	malicious	Browse	
	document-1370071295.xls	Get hash	malicious	Browse	
	document-69564892.xls	Get hash	malicious	Browse	
	document-1320073816.xls	Get hash	malicious	Browse	
	document-184653858.xls	Get hash	malicious	Browse	
	document-1729033050.xls	Get hash	malicious	Browse	
	document-540475316.xls	Get hash	malicious	Browse	
	document-1456634656.xls	Get hash	malicious	Browse	
	document-1376447212.xls	Get hash	malicious	Browse	
	document-1813856412.xls	Get hash	malicious	Browse	
	document-1776123548.xls	Get hash	malicious	Browse	
	document-684762271.xls	Get hash	malicious	Browse	
	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	
	document-779106205.xls	Get hash	malicious	Browse	
185.186.244.95	document-1048628209.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico
	document-1771131239.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico
	document-69564892.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico
	document-1813856412.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico
	document-1776123548.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico
	document-647734423.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico
	document-1579869720.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico
	document-806281169.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico
	document-839860086.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico
	document-1061603179.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico
	document-909428158.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico
	document-1822768538.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico
	document-1952275091.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico
	document-583955381.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico
	document-1312908141.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico
	document-1612462533.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1669060840.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-203135823.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-1042699213.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-980795635.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
urs-world.com	KAsJ2r4XYY.dll	Get hash	malicious	Browse	• 185.186.244.95
	swlsGbeQwT.dll	Get hash	malicious	Browse	• 185.186.244.95
	document-1048628209.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1771131239.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-69564892.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1729033050.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1813856412.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1776123548.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-647734423.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1579869720.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-895003104.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-779106205.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-806281169.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-839860086.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1061603179.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-909428158.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1747349663.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1822768538.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1952275091.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-583955381.xls	Get hash	malicious	Browse	• 185.186.244.95
under17.com	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-415601328.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-895003104.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-69633738.xls	Get hash	malicious	Browse	• 185.243.114.196

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ACCELERATED-ITDE	BnJvVt951o.exe	Get hash	malicious	Browse	• 152.89.236.214
	BnJvVt951o.exe	Get hash	malicious	Browse	• 152.89.236.214
	SMtbg7yHyR.exe	Get hash	malicious	Browse	• 152.89.236.214
	KAsJ2r4XYY.dll	Get hash	malicious	Browse	• 185.243.114.196
	swlsGbeQwT.dll	Get hash	malicious	Browse	• 185.243.114.196
	document-1048628209.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1771131239.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1370071295.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-69564892.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1320073816.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-184653858.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1729033050.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-540475316.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1456634656.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1376447212.xls	Get hash	malicious	Browse	• 185.243.114.196
	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
WEBZILLANL	document-1048628209.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1771131239.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-69564892.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1813856412.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1776123548.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-647734423.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1579869720.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-806281169.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-839860086.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1061603179.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-909428158.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1822768538.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1952275091.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-583955381.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1312908141.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1612462533.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1669060840.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-203135823.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1042699213.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-980795635.xls	Get hash	malicious	Browse	• 185.186.244.95

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{7FB5F6ED-9690-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7717358412536288
Encrypted:	false
SSDEEP:	48:IwhGcprkGwpLnG/ap8FT1GIpcFuSZGvnZpvFutZGoA1qp9FutXoGo4UcZpmFu1XT:rXZcZv2N3W0SGt0Pf0lVM0ty5AB
MD5:	C7ADC8FCAD859E4EA66F041590CEA754
SHA1:	DE539AD912690FFAF9D530B8D223F0AED8CC0A2D
SHA-256:	03053596FB8E95186650D6E1F7F8FE5A55BBCD326EDE3CFEC7217AC445DF4A8F
SHA-512:	5A8E73CD0E730BB80F9ACA77DCC9B4CC4DE36D0CACD2E9CB74708824ED832FE4555EA8293E78883E932D987600C91AFA5FF051B0C3A2B582402084352085780
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{9BF6741F-9690-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	50344
Entropy (8bit):	2.0044926127202616
Encrypted:	false
SSDEEP:	192:rTZgZ62JWitwfSxMdOvTlM52ThGM2Y3sg:rVw54a+zdOvC52EYX
MD5:	554821B70C1AABCB71236C098C6EE923
SHA1:	7F5337D277CE0AC68E54699205EA6FDAB7839B37
SHA-256:	7AE6415B9ADA174F4D6BF559F2BADB7B8458015A5D6BB769ADAF59B4E134D3D7
SHA-512:	20A13CADD9E55A8CFF06F3275C0C367B6125BDCA05D3A52735A2C5A1DE09ACFC1EA1EFEBA9CD6C09BA10F35F521F82F70B1C55DA30F3D24D988653AA6C50284
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{B2101CDB-9690-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33448
Entropy (8bit):	1.9155700208340736
Encrypted:	false
SSDEEP:	192:r4ZgZj2V9WVStV4fVIBMV+VDCV+hZMV+6:r4wauQ0bMwVR
MD5:	CA05CDF4541375AB4073A518D8E807CE
SHA1:	A5F5EC4C0923998210E75C05E31E8354EA7B0779
SHA-256:	A6C17D9BB935E6AB9984341CF31C3AE72846082774CF113FC7E40567ADB88B98
SHA-512:	6551053BB9E4BB74744257DFA15803696C4D0F30890F6A759C4C8A7183A66C65240C69A34E280F9D3917D647C9DDF2E98557C51A6278DF5B2F3005C9159C7811
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7FB5F6EF-9690-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	43324
Entropy (8bit):	2.5036770619245603
Encrypted:	false
SSDEEP:	384:rk8aGbw0OIsOfeQLfeQDZfeQ4feQqfeQPfeQmfTifTqfeQxfTlYfeQ/knfeQUV:WmZDZlZwZCZ3ZQTkTCZpTKZOZo
MD5:	CAE2162A5DFC24371121CE36C54B8A3E
SHA1:	C9D0653E2DAFAF48948FEA8B6FC6B72D893CABB1
SHA-256:	CB67C5FE43A0DD2C6DE93F59AB1BB3CC5545D11713FE20844101B44CB2B2DBF5
SHA-512:	AEBDCF2E6DCC7F8F0E68145E45238801E7650B8E8E5D60EE580153685418FDF740014E505BA1CE0D0067998DE9BC3C8C6E0B99B746952BA660217ED87F6F1BB
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9BF67421-9690-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27364
Entropy (8bit):	1.8384483667176679
Encrypted:	false
SSDEEP:	192:rbZYQi6wkRjp2pWqMGGc/4yZRc/4yX/qA:rtBN9t4Yrpa4yna4yvN
MD5:	ACF7EFA63FA34DFEA4E1BA8A41A89509
SHA1:	18491B3DEBD39AA12F765209FDC498D64FDF400F
SHA-256:	E298D82AD545C3669957F096AFBE9B949E3AF03C281CFAC8C38D15CE751CA0D8
SHA-512:	F2CD9B21D69F55126017D3103CEA10B26EB7BB0EB7ACC42FCF08FC2D9C9A5A033B4D3B3458768589C00E571DACE130DA653A9A4A5A1464DD2719A8C0BD7FF97
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9BF67423-9690-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	27864
Entropy (8bit):	1.824580676096497
Encrypted:	false
SSDEEP:	96:r2ZlQid6QBSTj1n2FWrMrSVlmqfgClRVlmqfgC2lmqrr:r2ZlQW6QkTj92FWrMrS2OR2Oar
MD5:	12A5873E9E2F6D563A308A14C61EA286
SHA1:	BF91E17014D0873DC4E6A9C6B4361D3B8FF1DCC2
SHA-256:	B311522455C26E0E334AE1AB7F7B80B8561D9A9F97F02CA4395791F478DE34E6
SHA-512:	727AC427261840C51A0DB2608DAA5B795D231DACCB3D4DBECF5A060EAD62323B63AF2006C3716D712DCDD972D9AF2336A1977965D8FFAB94A1E4599D22BEC67
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B2101CDD-9690-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5738161419033292
Encrypted:	false
SSDEEP:	48:IwJGcprnfGwpa60G4pQsmGrapbSqcGQpBx0xGHHpcxhTGUpG:rPZnpQ6E6soBSfjx0s2xjA
MD5:	94BDF460BB68ED333585F00ECB718C17
SHA1:	5958641DE66565D81E18B7A1E5BBC379AD6BDE65

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B2101CDD-9690-11EB-90E4-ECF4BB862DED}.dat	
SHA-256:	6274EE69DA9B50B4D4EF2D8CDE740DC6AB5FB63545FF9060F5542DE8BBEB178B
SHA-512:	6868C2AAE124DB001C7CADD2192197BE8E850AA35296B8A385EEE4FD3FFF19E195B5C85722EE9BEE55BA36E2C3082F552280FE386219F324D4460E80EE145AD F
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B2101CDF-9690-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5727161647940349
Encrypted:	false
SSDEEP:	48:IwUGcprdGwpa4G4pQ8GrapbSJGQpB+GHHpcqTGUpG:rIZHQo66BSDjN26A
MD5:	E426C3C62C0EA52B9B3A46918FB8E16E
SHA1:	0B7243962E437337D4BCDC8B91B63DFB2AAA6580
SHA-256:	621AC97024AF90D63CE65BB4068D841D843186A30F7C6E756529F1D9075BD532
SHA-512:	9083A057DAB1CC1A11C2B10CE74EAE2F27D649E7386EEFDB04C3893AC41AC467D29AE56C96B6468C378ED0048DDE2F1F74B08A47C25029F7F50AFA7ED827DI 7D
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	10192
Entropy (8bit):	4.53275317550241
Encrypted:	false
SSDEEP:	96:0Ph+Qhato4xrDehrmPPh+Qhato4xrDehrmi:0Z+dnVDehKPZ+dnVDehKi
MD5:	00B83F069ED2C79C4212EBB87CCEA3EB
SHA1:	FCE2899AAD94BCED85CBC040BCF3B1D87DB31C54
SHA-256:	74829A27B18970A0F0DED18596B19225A5AF8EAC5E81B834E7D857C6B5C8CFB1
SHA-512:	B5E1F69013D9E201A3897252711163AE5A9E6C6255A27EB6F43A8F804D2F9E8588FD2F8A92B5D0B60E60755178F4CA22621AF35D81EA076F8EA3B569FC880FEB
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\0W10PBUV\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\BJp5dDFvoQm12CHBfp4PC6aiyg4.gz[1].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\0W10PBUV\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:sYuYPXznb0DR7dw8QhlWTQrt7
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\0W10PBUV\NGDGShwgz5vCvyjNFyZiaPlHGCE.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	252
Entropy (8bit):	4.837090729138339
Encrypted:	false
SSDEEP:	6:qbLkyK4hImTzBwhLM1whA+XzFE8KSiQLGPQQgnaqza:IQD2IkzaLMGAMzDBVKY+ia
MD5:	1F62E9FDC6CA43F3FC2C4FA56856F368
SHA1:	75ADD74C4E04DB88023404099B9B4AAEA6437AE7
SHA-256:	E1436445696905DF9E8A225930F37015D0EF7160EB9A723BAFC3F9B798365DF6
SHA-512:	6AADAA42E0D86CAD3A44672A57C37ACBA3CB7F85E5104EB68FA44B845C0ED70B3085AA20A504A37DDEDEA7E847F2D53DB18B6455CDA69FB540847CEA6419CDBC
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\0W10PBUV\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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\0W10PBUV\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:	DBA7D04CDF199E68F04C2FECFDADE32C2E9EC20B4596097285188D96C0E87F40E3875F65F6B1FF5B567DCB7A27C3E9E8288A97EC881E00608E8C6798B24EF3F
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/P3LN8DHh0udC9Pbh8UHnw5FJ8R8.gz.js
Preview:	var Identity=Identity||{},ham_id_js_downloaded=!1;(function(n,t,i,r,u,f,e){e.wlProfile=function(){var r=sj_cook.get,u="WLS",t=r(u,"N"),i=r(u,"C");return i&&e.wlImgSm&&e.wlImgLg?{displayName:t?t.replace(/\+/g," "):"",name:n(t.replace(/\+/g," ")),img:e.wlImgSm.replace(/\{0\}/g,f(i)),imgL:e.wlImgLg.replace(/\{0\}/g,f(i)),idp:"WL"}:null};e.headerLoginMode=0;e.popupAuthenticate=function(n,i,r){var o,u,h,c,v=sb_gt(),l=Math.floor(v/1e3).toString(),s="ct",a=new RegExp("([?&])"+s+"=.*?(&|$)","i");return n.toString()==="WindowsLiveId"&&(o=e.popupLoginUrls,u=o[n],u=u.match(a)?u.replace(a,"$1"+s+"="+l+"$2"):u+"?"+s+"="+l,e.popupLoginUrls.WindowsLiveId=u),(o=e.popupLoginUrls)&&(u=o[n]+(i?"&perms="+f(i):"")+(r?"&src="+f(r):""))&&(h=e.pop(u))&&(c=setInterval(function(){h.closed&&(t.fire("id:popup:close"),clearInterval(c))},100))};e.pop=function(n){return r.open(n,"idl","location=no,menubar=no,resizable=no,scrollbars=yes,status=no,titlebar=no,toolbar=no,width=1000,height=620")};var o=u("id_h"),s=u("id

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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\0W10PBUV\Xp-HPHGHOZznHBwdn7OWdva404Y.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	576
Entropy (8bit):	5.192163014367754
Encrypted:	false
SSDEEP:	12:9mPi891gAseP24yXNbdPd1dPkelrR5MdKIKG/OgrfYc3tOfIvHbt:9mPlP5smDy1dV1dHrLMdKIKG/OgLYgtV
MD5:	F5712E664873FDE8EE9044F693CD2DB7
SHA1:	2A30817F3B99E3BE735F4F85BB66DD5EDF6A89F4
SHA-256:	1562669AD323019CDA49A6CF3BDDECE1672282E7275F9D963031B30EA845FFB2
SHA-512:	CA0EB961E52D37CAA75F0F22012C045876A8B1A69DB583FE3232EA6A7787A85BEABC282F104C9FD236DA9A500BA15FDF7BD83C1639BFD73EF8EB6A910B75290D
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/Xp-HPHGHOZznHBwdn7OWdva404Y.gz.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Xp-HPHGHOZznHBwdn7OWdva404Y.gz[1].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\0W10PBUV\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493 AC6D
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(); initMo reInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\k5oM71-Oyo7w7ptkcB_2S5dIr7I.gz[1].js	
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.defineProperty(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():"function"==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 instanceof 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\0W10PBUV\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\0W10PBUV\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\0W10PBUV\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\test[1].htm	
MD5:	E82D9BD501B46DF5CB2B650AF9E1B126
SHA1:	0FE6876226E88D8104ED51CB6329EB172BBA8D68
SHA-256:	C2BA8FCCFC980BCC8FC24E7A41BFCFEE88CCA9331C8D4D62890D7DFAB4A12226
SHA-512:	D3715E6A3C9012F2D8E1269E5C4B3E2F77FD2CD8E793AD39E51F1E1BE30F0818DDD01FAF3708EF789FDF347B92C6477C10A1155DEC582FF68185CBFD41C662 4
Malicious:	false
Preview:	IPv6Tests.TestIPv6Response('{"type": "4"}');

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\GiGr-rA9TBhE2c3LJn7PvDweiOo.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	374771
Entropy (8bit):	5.158592433297743
Encrypted:	false
SSDEEP:	6144:1irrzbB3LH7gaV6Z8LAfP0Rp6Izc04YFdNwRm2EjXi4SG7oIBYQmzeH:aHNfi4KwYQmzeH
MD5:	F279A46B56038C41BB3FC11D67D0FE46
SHA1:	B48121E695FD6483CAA7F48DE73FE9F121777109
SHA-256:	A9EA274B393E34591387AC0B4DE594BEE296386543DE34F4897281324DB0DCBB
SHA-512:	4C1754CF5E368D8CE86B135B789A4FF4BAAD1419F30A1EB3B65EAB62217C054D0066EA5FC22B5AA7643EA959854EBC2029B39CB7D1AEAAFB78B95A2A46430F 84
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/GiGr-rA9TBhE2c3LJn7PvDweiOo.gz.js
Preview:	(function(n){function t(r){if(i[r])return i[r].exports;var u=i[r]={i:r,l:!1,exports:{}};return n[r].call(u.exports,u,u.exports,t),u.l=!0,u.exports}var i={};return t.m=n,t.c=i,t.d=function(n,i,r){t.o(n,i)||Object.defineProperty(n,i,{enumerable:!0,get:r})},t.r=function(n){typeof Symbol!="undefined"&&Symbol.toStringTag&&Object.defineProperty(n,Symbol.toStringTag,{value:"Module"});Object.defineProperty(n,"__esModule",{value:!0})},t.t=function(n,i){var r,u;if((i&1&&(n=t(n)),i&8)||i&4&&typeof n=="object"&&n&&n.__esModule)return n;if(r=Object.create(null),t.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:n}),i&2&&typeof n!="string")for(u in n)t.d(r,u,function(t){return n[t]}.bind(null,u));return r},t.n=function(n){var i=n&&n.__esModule?function(){return n["default"]}:function(){return n};return t.d(i,"a",i),i},t.o=function(n,t){return Object.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\MEEXW4H4\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:	4798E4E1E907EAE161E67B9BAB42206CE0F22530871EEC63582161E29DD00D2D7034E7D12CB3FE56FFF673BC9BB01F0646F9CA5DAED288134CB25978EFBBEC F
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\MEEXW4H4\PxkopLP[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):	374
Entropy (8bit):	7.38103139101799
Encrypted:	false
SSDEEP:	6:XtKRM9nqzFECLYjPUDV7TyTiQLjYixVTb87e/u2lkXh6xkSFR9te3QweqZ:X1qDYjPIJubp87OnBrLqZ
MD5:	CBC86AF30F006045E0C749DB61F066A4
SHA1:	6B770B59F3727ABD1D86C8CA2953E957F36FBCAE
SHA-256:	DB7115603FBED15A5DDFC1A2054EF74EF2779328EA4590D6240102989497A6CB
SHA-512:	1FAAF34C36F18858AD21A914F1D0C5FF7B5BDAF8A09BD208CFC612E02FEED91F989776688D3F3A9B6BF555E9E53F7FDCA5517AD8F512375652C0DBD6B1C5C4 AC
Malicious:	false
Preview:	.....T.Mo.@...M..L.w..3.H;r.T.....k7d.. .3.)....]u{....947..i.x.SS.).er...U.....zF.(.....=@.u.....TU....T%9LOvJ..a.i4.E...t..{.....}G.s.7+.....)..Y.X6.....l.qc.^ .QX...R.F..];.m!..!^;3.HI.x.....5.v..Y....r..>.WA.H.r....{&...y{6V.-X.E.b.&.SF.1.Z.M.....T*.....k..F..^.Fd.~..g@...l;..x.M.8.z....x.....`.6M..../.....:.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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\MEEXW4H4\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:	5E21B6E184CBB0013DCCE174345DAC14BB64D391CCA3B253F73C7373253FDCA5E0BB297A0BD2FAD237E4F796895807660369680621C49C8F99DF428ED3218C9
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\MEEXW4H4\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=0
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\eaMqCdNxIXjLc0ATep7tsFkfmSA.gz[1].js	
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\MEEXW4H4\gDsOfTXNZVl18jxNDvhXqAdf2tM.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	1821
Entropy (8bit):	5.098212659804913
Encrypted:	false
SSDEEP:	48:0N3GKBel/r5+8cDYC1YvHIH6ayskysb6NccyskpY3Imqc+DkR:oGKBelzw8fCuoaay5ySSy5q3Mc+4R
MD5:	EC15EB7CBFBFAA68BB1DE04A28C80270
SHA1:	D2570D4CFF3139EA66D15799C9E67211F5A03B20
SHA-256:	810A85F1E705231989251F3EB52DAFF3F0ACEE09C703339C301A7CBD22CF8FE6
SHA-512:	077446A676E47447CB771A119CD0EC2EC168E65FED4579E663866D2846F51E93B47367518EB9D79E04EACE139CDFF043E1E28D64559412B4770388B2FEF96A21
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/gDsOfTXNZVl18jxNDvhXqAdf2tM.gz.js
Preview:	(function(){function b(e){var l=e[1],s=l&&_ge(l.vid);s&&(h=_ge("bnp.nid."+f),i=n.getAttribute("data-overlay")==="true"?!0:!1,c=n.getAttribute("data-setscroll")==="true"?!0:!1,k(),ClassUtil.removeClass(h,y),s.style.display="block",c&&d(),sj_evt.fire("bnp.notif.shown",s),i?nt():sj_evt.fire("McpDismissed"),u=_ge(w),t=_ge(v),t.focus(),r=_ge(p),u&&sj_be(u,o,tt),t&&sj_be(t,o,g))}var v="bnp_btn_accept",o="click",y="b_hide",p="cookie_preference",w="bnp_btn_preference",r,u,t,n=_ge("bnp_cookie_banner"),s=_ge("b_footer"),f=_w.bnp.pb_sttc.id,h,e,i,c,k=function(){var t=n&&n.getAttribute("data-position"),i=_ge("bnp_container");i&&t&&t.toLocaleLowerCase()=="top"&&(i.style.top=t+"px",i.style.bottom="auto")},d=function(){var i=_ge("bnp_container"),r=_ge("bnp_action_container"),n=_ge("bnp_content_desc"),u=_ge("bnp_title_container"),t;i&&r&&n&&u&&(t=i.offsetHeight-(r.offsetHeight+u.offsetHeight+130),n.style.maxHeight=t+"px",t<280&&(n.style.marginRight="-10px"))},g=function(t){ManagedCookiePreferenceActio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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.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\MEEXW4H4\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
SHA1:	C2CBDA98252249E9E1114D1D48679B493CBFA52D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\n8-O_KIRNSMPFWQWrGjn0BRH6SM.gz[1].js	
SHA-256:	9400DF53D61861DF8BCD0F53134DF500D58C02B61E65691F39F82659E780F403
SHA-512:	07032D7D9A55D3EA91F0C34C9CD504700095ED8A47E27269D2DDF5360E4CAC9D0FAD1E6BBFC40B79A3BF89AA00C39683388F690BB5196B40E5D662627A2C49 A
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\MEEXW4H4\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\MEEXW4H4\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:IczNJTX5oO6UdEmrZhLjhCmfWw
MD5:	6F4EBEE6F946368A02FCF8615CFF289A
SHA1:	FDB7A1DBFE702E4ACB2CE3859E6CD1627E908B47
SHA-256:	574BC892E7F45D4CD74153511B183DB04680551E80EB389ECD619950081852B2
SHA-512:	A37BE5349A4A802E46300CE7C4AF3A8D154BA7ED06C94F4DBE372920ACE25237E954094EEF60D3EF8C350F65761FD0A224A22A23AE31C7405F67896C1EDD3D 6
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].l..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\PSUEOSZZ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\MstqcgNaYngCBavkktAoSE0--po.gz[1].js	
SHA-512:	D070B9C415298A0F25234D1D7EAFB8BAE0D709590D3C806FCEAEC6631FDA37DFFCA40F785C86C4655AA075522E804B79A7843C647F1E98D97CCE599336DD9D9
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.onerror=function(){n.onerror=null;n.src="";n.alt=""},n.onload=function(){n.alt=i},n.src=t)}n()})()

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
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: #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\PSUEOSZZ\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\PSUEOSZZ\bLULVERLX4vU6bjspboNMw9vl_0.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	very short file (no magic)
Category:	downloaded
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A99
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/bLULVERLX4vU6bjspboNMw9vl_0.gz.js
Preview:	0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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....#+....l..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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 web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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:	D8DC8358727590A1ED74DC70356AEDC0499552C2DC0CD4F7A01853DD85CEB3AEAD5FBDC7C75D7DA36DB6AF2448CE5ABDFF64CEBDCA3533ECAD953C061A9 338E
Malicious:	false
IE Cache URL:	http://https://www.bing.com/sa/simg/favicon-2x.ico
Preview:	....(... ...@..... .....N...Sz..R...R...P. ..N..L..H..DG.....R6..U...U...S...R...P...N..L..I..F..B...7.....S6..V...V...U...S ...R...P...N..L..I..F..C...?..:z.....O...W...V...V...U...S...R...P...N..L..I..E..C...?...;..{7..q2$.....T..D ..]...S)..p6..J...R...P...N..L..I..E..B..>..;..z7..p2..f,X.....A..O#..N!..N!..N!..P$..q:...P...N..K..I..E..A..=..9..x5..n0..e,...5..... .....Ea.Z,..T$..T$..T

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\hqx6FcD0hjfzrON5oLgx2RMMD1s.gz[1].js	
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\PSUEOSZZ\lK_FmcR4naKX9hpIwfe9ify1hf4.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_FmcR4naKX9hpIwfe9ify1hf4.gz.js
Preview:	var __assign=this&&this.__assign||function(){return __assign=Object.assign||function(n){for(var t,r,i=1,u=arguments.length;i<u;i++){t=arguments[i];for(r in t)Object.prototype.hasOwnProperty.call(t,r)&&(n[r]=t[r])}return n},__assign.apply(this,arguments)},__rest=this&&this.__rest||function(n,t){var u={},r;for(var i in n)Object.prototype.hasOwnProperty.call(n,i)&&t.indexOf(i)<0&&(u[i]=n[i]);if(n!=null&&typeof Object.getOwnPropertySymbols=="function")for(r=0,i=Object.getOwnPropertySymbols(n);r<i.length;r++)t.indexOf(i[r])<0&&Object.prototype.propertyIsEnumerable.call(n,i[r])&&(u[i[r]]=n[i[r]]);return u},__spreadArrays=this&&this.__spreadArrays||function(){for(var i=0,n=0,r=arguments.length;n<r;n++)i+=arguments[n].length;for(var u=Array(i),f=0,n=0;n<r;n++)for(var e=arguments[n],t=0,o=e.length;t<o;t++,f++)u[f]=e[t];return u},__awaiter=this&&this.__awaiter||function(n,t,i,r){function u(n){return n instanceof i?n:new i(function(t){t(n)})}return new(i||(i=Promise))(function(i,f){function o(n){

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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\WJ8I2OL4\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:tI9mc4sl3WGPXN4x7ZguUz/KVqNFvneuFNH2N9wF+tC77LkeWVLKetCsYuwdOvX0:t41WeXNC1f3q/7H2DlZWYeIsrGYyKYx7
MD5:	4E67D347D439EEB1438AA8C0BF671B6B
SHA1:	E6BA86968328F78BF7BF03554793ACC4335DF1DD
SHA-256:	74DEB89D481050FD76A788660674BEA6C2A06B9272D19BC15F4732571502D94A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\5rqGloMo94v3vwNVR5OsxDNd8d0[1].svg	
SHA-512:	BE40E5C7BB0E9F4C1687FFDDBD1FC16F1D2B19B40AB4865BE81DD5CF5F2D8F469E090219A5814B8DAED3E2CD711D4532E648664BFA601D1FF7BBAA83392D30E
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/5rqGloMo94v3vwNVR5OsxDNd8d0.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 32 32"><title>UserSignedOutIcon</title><circle cx="16" cy="16" r="16" fill="#eee"/><path d="M12.73 13.1a3.271 3.271 0 1 1 3.27 3.2 3.237 3.237 0 0 1-3.27-3.2zm-2.73 9.069h1.088a4.91 4.91 0 0 1 9.818 0h1.094a5.884 5.884 0 0 0-3.738-5.434 4.238 4.238 0 0 0 2.1-3.635 4.366 4.366 0 0 0-8.73 0 4.238 4.238 0 0 0 2.1 3.635 5.878 5.878 0 0 0-3.732 5.434z" fill="#666"/><path fill="none" d="M0 0h32v32h-32z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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\WJ8I2OL4\Jl2vUSlEIqWjk-99MuYp4W74zvQ[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1529
Entropy (8bit):	4.135964697042234
Encrypted:	false
SSDEEP:	24:tVvnjuJOeUsc4wg5a2/gt+lm/3HljKR99U1TrD3ptYZ7GDlh6ml0jeI4dIwDq8rz:rn1edcjg5pm/lKRXU1TrD5tJf6mzjidJ
MD5:	6D8EF11CB1C03B39D9ED4E4C9A2190B9
SHA1:	265DAF51294422A5A393EF7D32E629E16EF8CEF4
SHA-256:	D72BEAE30A6B2B36C3E03847CE4EA04211D7373D4066FF937A7A05DF4E0C3DB6
SHA-512:	C8820BDF2FC34CCFF7018A1C1E3E74ED1FE0B287926050F9B6BA59C08DCC216E8732F862AB0BF086BC05275C51E6F81132AFA60F6D50A19585642BC906DCDD2
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/Jl2vUSlEIqWjk-99MuYp4W74zvQ.svg
Preview:	<svg width="16" height="16" viewBox="0 0 16 16" fill="none" xmlns="http://www.w3.org/2000/svg">..<path d="M8 0C6.41775 0 4.87103 0.469192 3.55544 1.34824C2.23985 2.22729 1.21447 3.47672 0.608967 4.93853C0.00346629 6.40034 -0.15496 8.00887 0.153721 9.56072C0.462403 11.1126 1.22433 12.538 2.34315 13.6569C3.46197 14.7757 4.88743 15.5376 6.43928 15.8463C7.99113 16.155 9.59966 15.9965 11.0615 15.391C12.5233 14.7855 13.7727 13.7602 14.6518 12.4446C15.5308 11.129 16 9.58225 16 8C16 5.87827 15.1571 3.84344 13.6569 2.34315C12.1566 0.842854 10.1217 0 8 0V0Z" fill="white"/>..<path d="M3.72395 9.60957L5.72394 11.6096C5.97398 11.8595 6.31306 12 6.66661 12C7.02016 12 7.35924 11.8595 7.60928 11.6096L12.2759 6.9429C12.4033 6.81991 12.5049 6.67278 12.5747 6.51011C12.6446 6.34744 12.6814 6.17248 12.6829 5.99544C12.6845 5.8184 12.6507 5.64283 12.5837 5.47897C12.5167 5.3151 12.4177 5.16623 12.2925 5.04104C12.1673 4.91585 12.0184 4.81685 11.8545 4.74981C11.6907 4.68277 11.5151 4.64903 11.3381 4.65057C11.16

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\MDr1f9aJs4rBVf1F5DAtlALvweY.gz[1].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\WJ8I2OL4\PA3TC2iNXZkiG2C3IJp5VAvC_yY.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	930
Entropy (8bit):	5.191402456846154
Encrypted:	false
SSDEEP:	24:GFUFqJYYmaLOTCE20aOtZP9F3a6MakIq+IvyUJ9sq5aOB:BWOWEZP9U6MHEvyUJ9s6
MD5:	73BFB9BB67A7271E257A4547007469A5
SHA1:	28F7B820679A99318E0DC596A54480D6AD5C3661
SHA-256:	A22BB5BD48C4C578C6BC4FDC4B8FF18F9162848F14E05AE283EC848B08EC8C15
SHA-512:	432142851A492C7635B764AC5293B6EFC943624FBD2FEA5D0F2D8900208B5F6233F5563B7CC08F314E29889B2628F298355484700816A3679F6A3315E63581F0
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/PA3TC2iNXZkiG2C3IJp5VAvC_yY.gz.js
Preview:	var ShareDialog;(function(n){function i(){t("bootstrap",arguments)}function r(){t("show",arguments)}function u(){t("showError",arguments)}function t(n,t){for(var r=["shdlgapi",n],i=0;i<t.length;i++)r.push(t[i]);sj_evt.fire.apply(null,r)}n.bootstrap=i;n.show=r;n.showError=u})(ShareDialog||(ShareDialog={})),function(n){function i(){t==0&&u()}function r(){sj_evt.unbind("shdlgapi",i)}function u(){t=1;var n=ShareDialogConfig.shareDialogUrl+"&IG="+_G.IG;n=e(n,["uncrunched","testhooks"]);sj_ajax(n,{callback:function(n,i){n?(t=2,i.appendTo(_d.body),r(),f()):t=3},timeout:0})}function f(){var n="rms";_w[n]&_w[n].start()}function e(n,t){var i,r,u;for(r in t)u=new RegExp("[?&]"+t[r]+"=[^?&#]*","i"),(i=location.href.match(u))&&i[0]&&(n+="&"+i[0].substring(1));return n}function o(){n.inited=0}function s(){n.inited||(n.inited=1,sj_evt.bind("shdlgapi",i,!0),sj_evt.bind("ajax.unload",o,!1))}var t=0;s()}(ShareDialog||(ShareDialog={}))

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\TXO4IVQH.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	60537
Entropy (8bit):	5.760642748679859
Encrypted:	false
SSDEEP:	1536:GUrSCXrLQvo3HJmcpUQEETOuKsIecFXdAjvdC94fJLYvX+8ab097Q53Opw:GwLQQ3pdmQJdC9RQew
MD5:	BDAC4671E46F60410AD36D9798A21557
SHA1:	83C306F3409CD5FD4188D2AA152E6FB626CBE2FC
SHA-256:	BC7866D2463C5D4D18E50A52D07B66239F6E73940E7B2B90D11A90D13E803955
SHA-512:	223326A4C079E2F3C01379A6EAD1AF1B56EDC1E75B6AD44005F0FE2D3E40BA7924F996BE65B46C00563BA287058785E9353DE25EC9093DB9A71994C0070F219A
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 into action, making it faster and easier to go from searching to doing." /><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta name="viewport" content="width=device-width, initial-scale=1.0" /><meta property="fb:app_id" content="570810223073062" /><meta property="og:type" content="website" /><meta property="og:title" content="Info" /><meta property="og:image" content="https://www.bing.com/th?id=OHR.SautduBrot_ROW9659507110_tmb.jpg&rf=" /><meta property="og:image:width" content="1366" /><meta property="og:image:height" content="768" /><meta property="og:url" content="https://www.bing.com/?form=HPFBBK&ssd=20210405_0700&mkt=de-CH" /><meta property="og:site_name" content="Bing" /><meta property="og:description" content="This stone bridge, known as Saut de Brot, looks li" /><title>Bing</title><link rel="shortcut ic

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\eRYlUYIMYsB_Pt8B7FTik-pl5cs.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	229
Entropy (8bit):	4.773871204083538
Encrypted:	false
SSDEEP:	3:2LGffIc6CaA5FSAGG4Aj6NhyII6RwZtSAnM+LAX6jUYkjdnwO6yJxWbMPJ/WrE6J:2LGXX6wFSADj6iIunnyh6TbMFsise2
MD5:	EEE26AAC05916E789B25E56157B2C712
SHA1:	5B35C3F44331CC91FC4BAB7D2D710C90E538BC8B
SHA-256:	249BCDCAA655BDEE9D61EDFF9D93544FA343E0C2B4DCA4EC4264AF2CB00216C2
SHA-512:	A664F5A91230C0715758416ADACEEAEFDC9E1A567A20A2331A476A82E08DF7268914DA2F085846A744B073011FD36B1FB47B8E4EED3A0C9F908790439C930538
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/eRYlUYIMYsB_Pt8B7FTik-pl5cs.gz.js
Preview:	(function(){var t=_ge("id_h"),n=_ge("langChange"),i=_ge("me_header"),r=_ge("langDId"),u=_ge("mapContainer");t!=null&&n!=null&&i==null&&(r===null||u===null)&&(t.insertBefore(n,t.firstChild),n.className=n.className+" langdisp")})()

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\errorPageStrings[1]	
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 conn ection.";..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 web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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.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\WJ8I2OL4\pXscrbCrewUD-UetJTvW5F7YMxo.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	511
Entropy (8bit):	4.980041296618112
Encrypted:	false
SSDEEP:	12:yWF4eguIWKvU9bEMsR5OErixCvJO1Vi5rgsM:LF4mKctEMYOK4CvJUVYM
MD5:	D6741608BA48E400A406ACA7F3464765
SHA1:	8961CA85AD82BB701436FFC64642833CFBAFF303
SHA-256:	B1DB1D8C0E5316D2C8A14E778B7220AC75ADAE5333A6D58BA7FD07F4E6EAA83C
SHA-512:	E85360DBBB0881792B86DCAF56789434152ED69E00A99202B880F19D551B8C78EEFF38A5836024F5D61DBC36818A39A921957F13FBF592BAAFD06ACB1AED244
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/pXscrbCrewUD-UetJTvW5F7YMxo.gz.js
Preview:	var BingAtWork;(function(n){var t;(function(n){function t(t,i){var u,r;t.isAuthenticated&&(n.raiseAuthEventAndLog(t),u=_ge("sb_form_q"),u&&(r=u.getAttribute("value"),r&&(n.fetchLowerHeader(r),n.fetchScopeBar(r),i.notifEnabled&&i.notifFetchAsync&&n.fetchNotificationConditional())))}function i(n,i){n&&n.length==2&&t(n[1],i)}n.bind ToConditionalSignIn=function(n){sj_evt.bind("ssofirstquery",function(t){return i(t,n)},!0,null,!1)}})(t=n.ConditionalSignIn||(n.ConditionalSignIn={}))})(BingAtWork||(Bing AtWork={}))

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\sTWC0LplwPyIP_jw8VjHps800ZQ.gz[1].js	
SSDEEP:	384:+WLj/9N/zdUjP+c4QQKaK9JASETkyWJLhjO4YuiqRqNlRxW+:+u/P/zdUraOJhaShK1uiqR0T3
MD5:	44AD44162E25A1DB1F46F78B8ECFAD42
SHA1:	C63A0E7B132221D572A541F700601356627A98A4
SHA-256:	5AE500A4737BE7B187EEA99AAB81CF3D4796D23550F7C5349DE2430E6624918D
SHA-512:	4F0078431E86CCD8C0B3DE7E4F7CC10B184DC5376AD10C224EC081DAE1B9D16509E01A95CE3F3B4F7C394EC2C52782E4CB9AC2DE8C12CA0FFC9CC66C01C5AFD
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"],function(n,t){function s(n,t){for(var r=n.length,i=0;i<r;i++)t(n[i])}function r(n){for(var i=[],t=1;t<arguments.length;t++)i[t-1]=arguments[t];return function(){n.apply(null,i)}}function u(n){i&&event&&(event.returnValue=!1);n&&typeof n.preventDefault=="function"&&n.preventDefault()}function f(n){i&&event&&(event.cancelBubble=!0);n&&typeof n.stopPropagation=="function"&&n.stopPropagation()}function e(n,t,i){for(var r=0;n&&n.offsetParent&&n!=(i||document.body);)r+=n["offset"+t],n=n.offsetParent;return r}function o(){return(new Date).getTime()}function h(n){return i?event:n}function c(n){return i?event?event.srcElement:null:n.target}function l(n){return i?event?event.fromElement:null:n.relatedTarget}function a(n){return i?event?event.toElement:null:n.relatedTarget}function v(n,t,i){while(n&&n!=(i||document.body)){if(n==t)return!0;n=n.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\swyt_VnIjJDWZW5KEq7a8l_1AEw.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2298
Entropy (8bit):	5.34865319631632
Encrypted:	false
SSDEEP:	48:KWEkTScZVcMBOwXhzwBi88RnX8ec0T39B8onA008xG9FLCx3w0S5xJ:KWEkTDZVXpR0BiXjTtB8mA0zxWsx3PG/
MD5:	A8D7D1B3681590980B2D7480906078DB
SHA1:	C9A7A400DB1EBAD4DCA028546EE5F5B2EF4136BD
SHA-256:	1390485DC88B6230389D9C95232A3710BF38D47271708A279B12D7E68E43F649
SHA-512:	710D31EFD76614EC4C94888E2FCC49ABAB50EF406FC0F1C5C10D8AA21D4E9F349DE78068B2BAFE495C074AB4E6EC0A5D44EB5506B2D79C78707A23C1D820664
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\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.395590914706752
Encrypted:	false
SSDEEP:	3:oVXU16m/yMW8JOGXnE16m/yBn:o9Uv/yBqEv/yB
MD5:	BF241D7DCC250DB274F7573443339763
SHA1:	0290C5B8B14FF971FC566C8CB41E079CAA727AFB
SHA-256:	092FD9B90847DE35DBDA4683CC1CEBF3096A089F896A643D3CE4BBF04DCF2EE7
SHA-512:	5F263DF73B5566707E8D2BD5723C9EC8543ADE85AE595F542EA74AE6E5CE473863C3B370D4DDB1E364FD2F3F03C4EE65F69B4C4D17B75658951817020B60D6F
Malicious:	false
Preview:	[2021/04/05 21:29:02.163] Latest deploy version: ..[2021/04/05 21:29:02.163] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF058AFC2113F0053A.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39625
Entropy (8bit):	0.5636841358055481
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+6cGPcmcIFQ4FK4ajcIFQ4FK4aDcIFQ4FK4ao:kBqoxKAuqR+6cGPcmc/4yjc/4yDc/4yo
MD5:	D6AD526DD03F6773F983A3105AA949D3
SHA1:	04A95E53490FFE58FB7F25599BA189516006B13D
SHA-256:	AECBFCB9E873A3BD96CE50349413DF931F3257FBEFC614A3272B2F3A01983913
SHA-512:	E21975587B52CE092DBFC02D67DFD70649AB093291D8B1F3B4BF232334105338A166DE7B4D11E0BA18351708F6648A1DC94D8DA9D84B23441CB2526BB9E7386
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DF058AFC2113F0053A.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF0C0AB4E01F910CE6.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25657
Entropy (8bit):	0.313669193592156
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwxi9lwxy9l2x9:kBqoxKAuvScS+xlxLx9
MD5:	1CBA300DC9AE546ADFC1203AACEFF07A
SHA1:	61D51960E86AF008555A42945478C4C80B02E18F
SHA-256:	04884926F91BD15DC467E05AD087793E68E28C6FA66258B43A8CA3E30B63DF24
SHA-512:	393B738FA415A7636D3FDE5D8B53EAACF6B29791160EFF0C7177F00904A2E7DDDF7CB7DC0FB8100878DC505095B97C86CBDB544A86B188C9ED00594C160E88 8
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF192FA70C64A9B1B3.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39601
Entropy (8bit):	0.5635865533671768
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+vRT6h7VlmqfgCRVlmqfgCtVlmqfgCS:kBqoxKAuqR+vRT6h72A2w2h
MD5:	1F7685E1F420E8ED132445097A1E5CFB
SHA1:	1C60E122B24447D325663212806B6C60CE9B0775
SHA-256:	122EFE7D17CCFC5940AFC861FDCC57D0BB7E2AE44CBC0E61F776C47777C378C7
SHA-512:	08AC55DAC30EF8D570C246A1FA694A5DCEFC5B6CA9487CCC1BD2454BDFD1DBF29D449A2C8A3C4F7A80C2913D1BA7454111E35EDA560D41B61D07533724820 72
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF38505126371D5564.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	53618
Entropy (8bit):	1.5798945781140086
Encrypted:	false
SSDEEP:	768:VmZsZlZwZCZ3ZQTkTCZpTaZSZ6ZZ3KIiy:VnTiy
MD5:	A5A782055AD36C3D6488FEE811DD3CC5
SHA1:	6394BE47BF1DB0A3580181BA2E287734FFDF21D8
SHA-256:	0401AE4477AA1D36BB8CC4765464E24E7848179C15B314F397D7C48617ED2685
SHA-512:	E43B679B7A38AD893CF381D6E2AFB525FC686CD02ECD2C2A20BE6FB0C6A62417DBDC1CE438BAA1EA6F0B3B6506DEEFBF8B6546AD8E4E7B2B4192705D36560 80E
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF54D02285566ED38C.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Temp\~DF54D02285566ED38C.TMP	
Size (bytes):	25657
Entropy (8bit):	0.31313648665196103
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwE9lw09l2X:kBqoxKAuvScS+XZX
MD5:	9D2F8FF8132F67616BA99BAAC5705C15
SHA1:	0D4F17625F9CB34C1CF3EC8B0BFA69E653BC335F
SHA-256:	D0EA4803928A523667113FC6071DCE2E4AC9F775A3E3D26C34420B8AB4764AC1
SHA-512:	578CC569FE8D75ECCE5891C8F1CF4440E5863E6F0CECF8483C94A0CC4C0D0BB4DAD1532BE87C97089B8B449A555A737225400972643ADDE8875507BF94D315
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF6BD6E167C9C7F1E2.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13237
Entropy (8bit):	0.5966582493194083
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loWF9loa9lWDs1l51PO1PpnPpmyC:kBqoI1jDUP5O5hI
MD5:	1ECBE96230A4816D22D6B49836E1ED63
SHA1:	9892FE431C70865263037C806FB65A2DA7AB9575
SHA-256:	651A83EEA796E1DCD63455E7F71C4D351EF0E1DEE093F8C5C5B44160C703FB15
SHA-512:	66512716268255F8899799990C391C1878BD6F99F87C00EA523D582677C6CE9EAD9C4F53AC42794C13D3FF4DC6E413CC99AF1E00255E50054E55A8429BD965C2
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFA05500DBA7D079FC.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13141
Entropy (8bit):	0.5378917421752247
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loZF9lo79lWVwxvbxbXxU:kBqoI8CVwxvbx7xU
MD5:	517313CA08585236853C4095FAEB0A6D
SHA1:	D2C2A5D12189382778E6B3B9747AF13BA4920014
SHA-256:	DCCAAB625905489FA60C8904DC63A86864A57561FFEC27E9A2E4ADB2F8D86030
SHA-512:	1D4A0970EC4494352D31CC8ABEB53FB45C758C21B225E9871C6DE8FE63D4860CCF58699383FD51383146C3847894ECAD551E8751FFA3041709AFBEF92805B0B
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFACC10D909317CF6D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.40671045950774876
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lovF9lot9lWFO7G:kBqoIWoFO7G
MD5:	B8B084DD0D0086433BCEB1E9350421AA
SHA1:	F67FDF78C87F18D45861A235768E605ADA0608D8
SHA-256:	0ED23F8178269AAAA9D4823A433C07F84637882D03D7B5D8F1F170520DD4F769
SHA-512:	FF4CB2D360FA013EE75058E6053A5CD16427EC3BEB3A7A0E6E84C4BEADD79610EA69B017BA57139850F4802D162341D8A4E040F30AA9067A3E562BDFA4D6BA FC
Malicious:	false

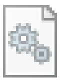
C:\Users\user\AppData\Local\Temp\~DFACC10D909317CF6D.TMP	
Preview:	.............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Wi ndows
Entropy (8bit):	5.758956237742167
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:	bTjvWUTLid.dll
File size:	108638
MD5:	9064c426999ab9e059e1e533b34f97be
SHA1:	cc20039678658d4e79aef801907f4a1bf06c418a
SHA256:	7d80947ba6784330e792fae5eded56f2e7f228740e19f9af 19106886e567b268
SHA512:	90ecf2795f387f2b3e3342e5e8185a5241df3869f0976b64 1cadbd0ee0f0629669774a8b3c818d85d438d629fe99764 4730412b1c9d6cc16e7101ad2346f0c7e
SSDEEP:	1536:DWKaY5Se9WnVI78XvnoxJasJvRHKmyGDvDk0 Rt9Y56l5ZMpvV05o9OX5xPw8:DWa0eQnVI7qCqZGDv Dk4wol5w0EU
File Content Preview:	MZ......................@...!..L.!Th is 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

Instruction
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 00007F6404B30300h
push ecx
add dword ptr [esp], 00000247h
sub dword ptr [esp], ecx
push ecx
mov dword ptr [esp], 00005267h
call 00007F6404B2CCA9h
push esi
mov esi, eax
or esi, eax
mov eax, esi
pop esi
jne 00007F6404B31DA2h
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 00007F6404B31D7Eh
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

Instruction
cld
rep movsb
push ebx
mov dword ptr [eax+eax], 00000000h

Data Directories

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

Sections

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

Imports

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

Exports

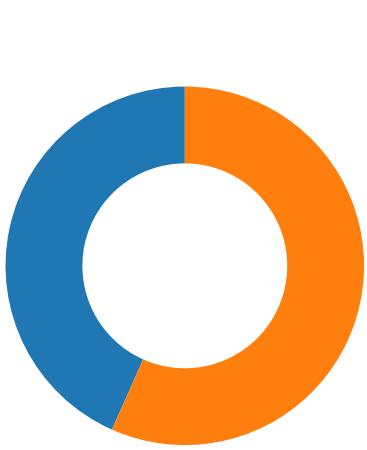
Name	Ordinal	Address
StartService	1	0x1000b959

Network Behavior

Network Port Distribution

Total Packets: 90

- 53 (DNS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 5, 2021 21:29:02.642251015 CEST	49761	80	192.168.2.3	185.243.114.196
Apr 5, 2021 21:29:02.642252922 CEST	49760	80	192.168.2.3	185.243.114.196
Apr 5, 2021 21:29:03.655380011 CEST	49761	80	192.168.2.3	185.243.114.196
Apr 5, 2021 21:29:03.655488968 CEST	49760	80	192.168.2.3	185.243.114.196
Apr 5, 2021 21:29:05.655420065 CEST	49761	80	192.168.2.3	185.243.114.196
Apr 5, 2021 21:29:05.656776905 CEST	49760	80	192.168.2.3	185.243.114.196
Apr 5, 2021 21:29:09.664412975 CEST	49762	80	192.168.2.3	185.243.114.196
Apr 5, 2021 21:29:09.679650068 CEST	49763	80	192.168.2.3	185.243.114.196
Apr 5, 2021 21:29:09.850311995 CEST	49765	80	192.168.2.3	185.243.114.196
Apr 5, 2021 21:29:09.850316048 CEST	49764	80	192.168.2.3	185.243.114.196
Apr 5, 2021 21:29:10.671564102 CEST	49762	80	192.168.2.3	185.243.114.196
Apr 5, 2021 21:29:10.687143087 CEST	49763	80	192.168.2.3	185.243.114.196
Apr 5, 2021 21:29:10.859096050 CEST	49764	80	192.168.2.3	185.243.114.196
Apr 5, 2021 21:29:10.859566927 CEST	49765	80	192.168.2.3	185.243.114.196
Apr 5, 2021 21:29:12.671648979 CEST	49762	80	192.168.2.3	185.243.114.196
Apr 5, 2021 21:29:12.687596083 CEST	49763	80	192.168.2.3	185.243.114.196
Apr 5, 2021 21:29:12.859265089 CEST	49764	80	192.168.2.3	185.243.114.196
Apr 5, 2021 21:29:12.859405041 CEST	49765	80	192.168.2.3	185.243.114.196
Apr 5, 2021 21:29:39.809091091 CEST	49769	80	192.168.2.3	185.186.244.95
Apr 5, 2021 21:29:39.809299946 CEST	49770	80	192.168.2.3	185.186.244.95
Apr 5, 2021 21:29:40.533814907 CEST	49772	80	192.168.2.3	185.186.244.95
Apr 5, 2021 21:29:40.534030914 CEST	49771	80	192.168.2.3	185.186.244.95
Apr 5, 2021 21:29:40.814666033 CEST	49769	80	192.168.2.3	185.186.244.95
Apr 5, 2021 21:29:40.814677954 CEST	49770	80	192.168.2.3	185.186.244.95
Apr 5, 2021 21:29:41.533401012 CEST	49772	80	192.168.2.3	185.186.244.95
Apr 5, 2021 21:29:41.548995972 CEST	49771	80	192.168.2.3	185.186.244.95
Apr 5, 2021 21:29:42.814883947 CEST	49770	80	192.168.2.3	185.186.244.95
Apr 5, 2021 21:29:42.814884901 CEST	49769	80	192.168.2.3	185.186.244.95
Apr 5, 2021 21:29:43.533556938 CEST	49772	80	192.168.2.3	185.186.244.95
Apr 5, 2021 21:29:43.549180031 CEST	49771	80	192.168.2.3	185.186.244.95
Apr 5, 2021 21:29:46.818007946 CEST	49773	80	192.168.2.3	185.186.244.95
Apr 5, 2021 21:29:47.534502983 CEST	49774	80	192.168.2.3	185.186.244.95
Apr 5, 2021 21:29:47.565860033 CEST	49775	80	192.168.2.3	185.186.244.95
Apr 5, 2021 21:29:47.830806971 CEST	49773	80	192.168.2.3	185.186.244.95
Apr 5, 2021 21:29:48.549617052 CEST	49774	80	192.168.2.3	185.186.244.95
Apr 5, 2021 21:29:48.565202951 CEST	49775	80	192.168.2.3	185.186.244.95
Apr 5, 2021 21:29:49.831526995 CEST	49773	80	192.168.2.3	185.186.244.95
Apr 5, 2021 21:29:50.565406084 CEST	49774	80	192.168.2.3	185.186.244.95
Apr 5, 2021 21:29:50.565450907 CEST	49775	80	192.168.2.3	185.186.244.95

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 5, 2021 21:27:36.114995956 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:27:36.163944006 CEST	53	55984	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 5, 2021 21:27:37.134896040 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:27:37.191584110 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 5, 2021 21:27:37.618683100 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:27:37.677021027 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 5, 2021 21:27:38.540122032 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:27:38.586324930 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 5, 2021 21:27:39.558151960 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:27:39.604132891 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 5, 2021 21:27:40.640930891 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:27:40.689701080 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 5, 2021 21:27:41.797220945 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:27:41.843223095 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 5, 2021 21:27:42.745155096 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:27:42.802537918 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 5, 2021 21:27:43.726969957 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:27:43.776957035 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 5, 2021 21:27:46.715800047 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:27:46.773454905 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 5, 2021 21:27:48.164750099 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:27:48.210689068 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 5, 2021 21:27:49.436039925 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:27:49.493580103 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 5, 2021 21:27:50.898350000 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:27:50.944279909 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 5, 2021 21:27:51.897588968 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:27:51.951991081 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 5, 2021 21:27:52.865010977 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:27:52.913676977 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 5, 2021 21:27:53.809218884 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:27:53.858067036 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 5, 2021 21:27:54.754987001 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:27:54.800981045 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 5, 2021 21:27:55.705811024 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:27:55.765067101 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 5, 2021 21:27:56.685452938 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:27:56.731561899 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 5, 2021 21:28:12.552906036 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:28:12.598908901 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 5, 2021 21:28:13.627759933 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:28:13.684211016 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 5, 2021 21:28:14.061445951 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:28:14.118000031 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 5, 2021 21:28:15.638549089 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:28:15.684504986 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 5, 2021 21:28:15.945755959 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:28:16.000439882 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 5, 2021 21:28:17.307054043 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:28:17.352893114 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 5, 2021 21:28:17.415981054 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:28:17.462059975 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 5, 2021 21:28:20.409178019 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:28:20.455291986 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 5, 2021 21:28:32.304845095 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:28:32.339781046 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:28:32.361129999 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 5, 2021 21:28:32.415014029 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 5, 2021 21:28:32.969791889 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:28:33.024785042 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 5, 2021 21:28:33.120146036 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:28:33.174561024 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 5, 2021 21:28:44.028485060 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:28:44.076163054 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 5, 2021 21:28:45.013696909 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:28:45.068003893 CEST	53	52123	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 5, 2021 21:28:46.031050920 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:28:46.085617065 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 5, 2021 21:28:47.728451967 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:28:47.786787033 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 5, 2021 21:28:48.048985004 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:28:48.095041990 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 5, 2021 21:28:52.061073065 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:28:52.107043982 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 5, 2021 21:28:55.466810942 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:28:55.530673981 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 5, 2021 21:29:01.376065969 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:29:01.432570934 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 5, 2021 21:29:02.562619925 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:29:02.629647017 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 5, 2021 21:29:09.763767004 CEST	63978	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:29:09.838340998 CEST	53	63978	8.8.8.8	192.168.2.3
Apr 5, 2021 21:29:16.706191063 CEST	62938	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:29:16.752425909 CEST	53	62938	8.8.8.8	192.168.2.3
Apr 5, 2021 21:29:16.875833988 CEST	55708	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:29:16.932018042 CEST	53	55708	8.8.8.8	192.168.2.3
Apr 5, 2021 21:29:18.979036093 CEST	56803	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:29:19.026993036 CEST	53	56803	8.8.8.8	192.168.2.3
Apr 5, 2021 21:29:19.436791897 CEST	57145	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:29:19.498889923 CEST	53	57145	8.8.8.8	192.168.2.3
Apr 5, 2021 21:29:36.507883072 CEST	55359	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:29:36.553900003 CEST	53	55359	8.8.8.8	192.168.2.3
Apr 5, 2021 21:29:38.523240089 CEST	58306	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:29:38.581756115 CEST	53	58306	8.8.8.8	192.168.2.3
Apr 5, 2021 21:29:39.683372021 CEST	64124	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:29:39.790157080 CEST	53	64124	8.8.8.8	192.168.2.3
Apr 5, 2021 21:29:40.466511965 CEST	49361	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:29:40.523974895 CEST	53	49361	8.8.8.8	192.168.2.3
Apr 5, 2021 21:29:53.834362030 CEST	63150	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:29:53.891289949 CEST	53	63150	8.8.8.8	192.168.2.3
Apr 5, 2021 21:29:54.570554018 CEST	53279	53	192.168.2.3	8.8.8.8
Apr 5, 2021 21:29:54.624902010 CEST	53	53279	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 5, 2021 21:28:17.307054043 CEST	192.168.2.3	8.8.8.8	0xe875	Standard query (0)	login.micr osoftonline.com	A (IP address)	IN (0x0001)
Apr 5, 2021 21:29:02.562619925 CEST	192.168.2.3	8.8.8.8	0xb13f	Standard query (0)	under17.com	A (IP address)	IN (0x0001)
Apr 5, 2021 21:29:09.763767004 CEST	192.168.2.3	8.8.8.8	0x7c57	Standard query (0)	under17.com	A (IP address)	IN (0x0001)
Apr 5, 2021 21:29:16.706191063 CEST	192.168.2.3	8.8.8.8	0x3c2a	Standard query (0)	under17.com	A (IP address)	IN (0x0001)
Apr 5, 2021 21:29:16.875833988 CEST	192.168.2.3	8.8.8.8	0x5468	Standard query (0)	under17.com	A (IP address)	IN (0x0001)
Apr 5, 2021 21:29:39.683372021 CEST	192.168.2.3	8.8.8.8	0x9f35	Standard query (0)	urs-world.com	A (IP address)	IN (0x0001)
Apr 5, 2021 21:29:40.466511965 CEST	192.168.2.3	8.8.8.8	0xd040	Standard query (0)	urs-world.com	A (IP address)	IN (0x0001)
Apr 5, 2021 21:29:53.834362030 CEST	192.168.2.3	8.8.8.8	0xac0f	Standard query (0)	urs-world.com	A (IP address)	IN (0x0001)
Apr 5, 2021 21:29:54.570554018 CEST	192.168.2.3	8.8.8.8	0xb6c5	Standard query (0)	urs-world.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 5, 2021 21:28:17.352893114 CEST	8.8.8.8	192.168.2.3	0xe875	No error (0)	login.micr osoftonline.com	a.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Apr 5, 2021 21:28:17.352893114 CEST	8.8.8.8	192.168.2.3	0xe875	No error (0)	a.privatel ink.msiden tity.com	prda.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 5, 2021 21:28:17.352893114 CEST	8.8.8.8	192.168.2.3	0xe875	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 5, 2021 21:28:17.462059975 CEST	8.8.8.8	192.168.2.3	0x1220	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 5, 2021 21:29:02.629647017 CEST	8.8.8.8	192.168.2.3	0xb13f	No error (0)	under17.com		185.243.114.196	A (IP address)	IN (0x0001)
Apr 5, 2021 21:29:09.838340998 CEST	8.8.8.8	192.168.2.3	0x7c57	No error (0)	under17.com		185.243.114.196	A (IP address)	IN (0x0001)
Apr 5, 2021 21:29:16.752425909 CEST	8.8.8.8	192.168.2.3	0x3c2a	No error (0)	under17.com		185.243.114.196	A (IP address)	IN (0x0001)
Apr 5, 2021 21:29:16.932018042 CEST	8.8.8.8	192.168.2.3	0x5468	No error (0)	under17.com		185.243.114.196	A (IP address)	IN (0x0001)
Apr 5, 2021 21:29:39.790157080 CEST	8.8.8.8	192.168.2.3	0x9f35	No error (0)	urs-world.com		185.186.244.95	A (IP address)	IN (0x0001)
Apr 5, 2021 21:29:40.523974895 CEST	8.8.8.8	192.168.2.3	0xd040	No error (0)	urs-world.com		185.186.244.95	A (IP address)	IN (0x0001)
Apr 5, 2021 21:29:53.891289949 CEST	8.8.8.8	192.168.2.3	0xac0f	No error (0)	urs-world.com		185.186.244.95	A (IP address)	IN (0x0001)
Apr 5, 2021 21:29:54.624902010 CEST	8.8.8.8	192.168.2.3	0xb6c5	No error (0)	urs-world.com		185.186.244.95	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: loaddll32.exe PID: 4740 Parent PID: 5840

General

Start time:	21:27:43
Start date:	05/04/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\bTjvWUTLid.dll'
Imagebase:	0x3a0000
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: 00000001.00000003.322688241.0000000003C4B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000002.468904575.0000000003A4F000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.322716434.0000000003C4B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000001.00000002.466547139.0000000000FE0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.322780684.0000000003C4B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.322817865.0000000003C4B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.402234739.0000000003B4D000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.322646205.0000000003C4B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.322756928.0000000003C4B000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 5936 Parent PID: 4740

General

Start time:	21:27:43
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\bTjvWUTLid.dll',#1
Imagebase:	0xbd0000
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: 6076 Parent PID: 4740

General

Start time:	21:27:44
Start date:	05/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\bTjvWUTLid.dll,StartService
Imagebase:	0x990000
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: 00000003.00000002.239107986.0000000002B20000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 4700 Parent PID: 5936

General

Start time:	21:27:44
Start date:	05/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\bTjvWUTLid.dll',#1
Imagebase:	0x990000
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: 00000004.00000003.294061363.0000000005418000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.293962458.0000000005418000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.293989967.0000000005418000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.294041063.0000000005418000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.294103973.0000000005418000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.294092748.0000000005418000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.294077737.0000000005418000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000002.469869205.0000000005418000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000002.468243030.00000000030B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.294019471.0000000005418000.00000004.00000040.sdmp, Author: Joe Security

Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 2296 Parent PID: 792

General

Start time:	21:28:13
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:	0x7ff70a730000
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	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 6212 Parent PID: 2296

General

Start time:	21:28:14
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:2296 CREDAT:17410 /prefetch:2
Imagebase:	0xb0000
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: 6356 Parent PID: 792

General

Start time:	21:29:00
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:	0x7ff64cbb0000
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: 6380 Parent PID: 6356

General

Start time:	21:29:01
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:6356 CREDAT:17410 /prefetch:2
Imagebase:	0xf0000
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: 1328 Parent PID: 6356

General

Start time:	21:29:07
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:6356 CREDAT:82952 /prefetch:2
Imagebase:	0xf0000
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: 6652 Parent PID: 792

General

Start time:	21:29:37
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:	0x7ff64cbb0000
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: 5024 Parent PID: 6652

General

Start time:	21:29:38
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:6652 CREDAT:17410 /prefetch:2
Imagebase:	0xf0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6584 Parent PID: 6652

General

Start time:	21:29:39
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:6652 CREDAT:17414 /prefetch:2
Imagebase:	0xf0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis