ID: 382555
Sample Name: gg.gif.dll
Cookbook: default.jbs
Time: 09:50:06
Date: 06/04/2021
Version: 31.0.0 Emerald

Table of Contents

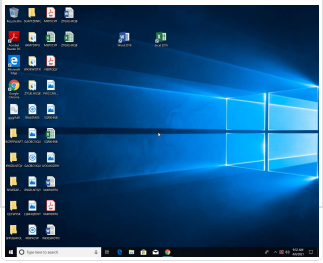
Analysis Report gg.gif.dll

Overview

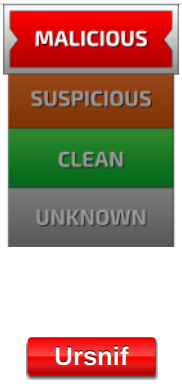
General Information

Sample Name:	gg.gif.dll
Analysis ID:	382555
MD5:	75ffb2cb4faff68f2..
SHA1:	543803cbfad26ff…
SHA256:	db9ede8dfbecb23.
Tags:	dll GG Gozi ISFB Ursnif
Infos:	

Most interesting Screenshot:



Detection

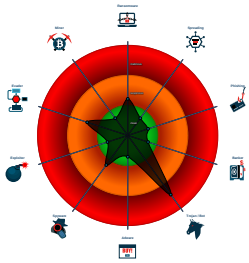


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6768 cmdline: loaddll32.exe 'C:\Users\user\Desktop\gg.gif.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6776 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\gg.gif.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6796 cmdline: rundll32.exe 'C:\Users\user\Desktop\gg.gif.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6784 cmdline: rundll32.exe C:\Users\user\Desktop\gg.gif.dll,StartService MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 7104 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 64 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7104 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 4732 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7104 CREDAT:82948 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 4864 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6196 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4864 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 7112 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4864 CREDAT:17414 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 1364 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6152 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1364 CREDAT:17410 /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
00000003.00000003.796910446.000000000507B000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.796966176.000000000507B000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000002.924347640.0000000004E7F000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000002.922918490.0000000001020000.00000004.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000000.00000003.797626012.00000000037EB000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 16 entries				

Unpacked PEs

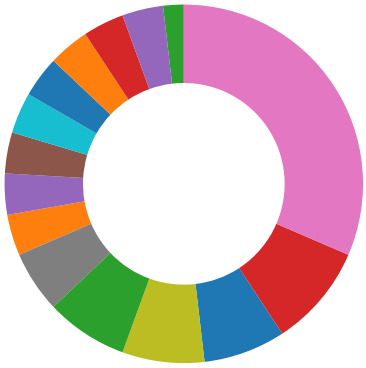
Source	Rule	Description	Author	Strings
2.2.rundll32.exe.2fb0000.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.2.rundll32.exe.10000000.5.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.loaddll32.exe.1020000.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.2.rundll32.exe.2c70000.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.loaddll32.exe.10000000.4.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Compliance
- Spreading
- Networking



- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

Yara detected Ursnif

System Summary:

Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

Yara detected Ursnif

Remote Access Functionality:

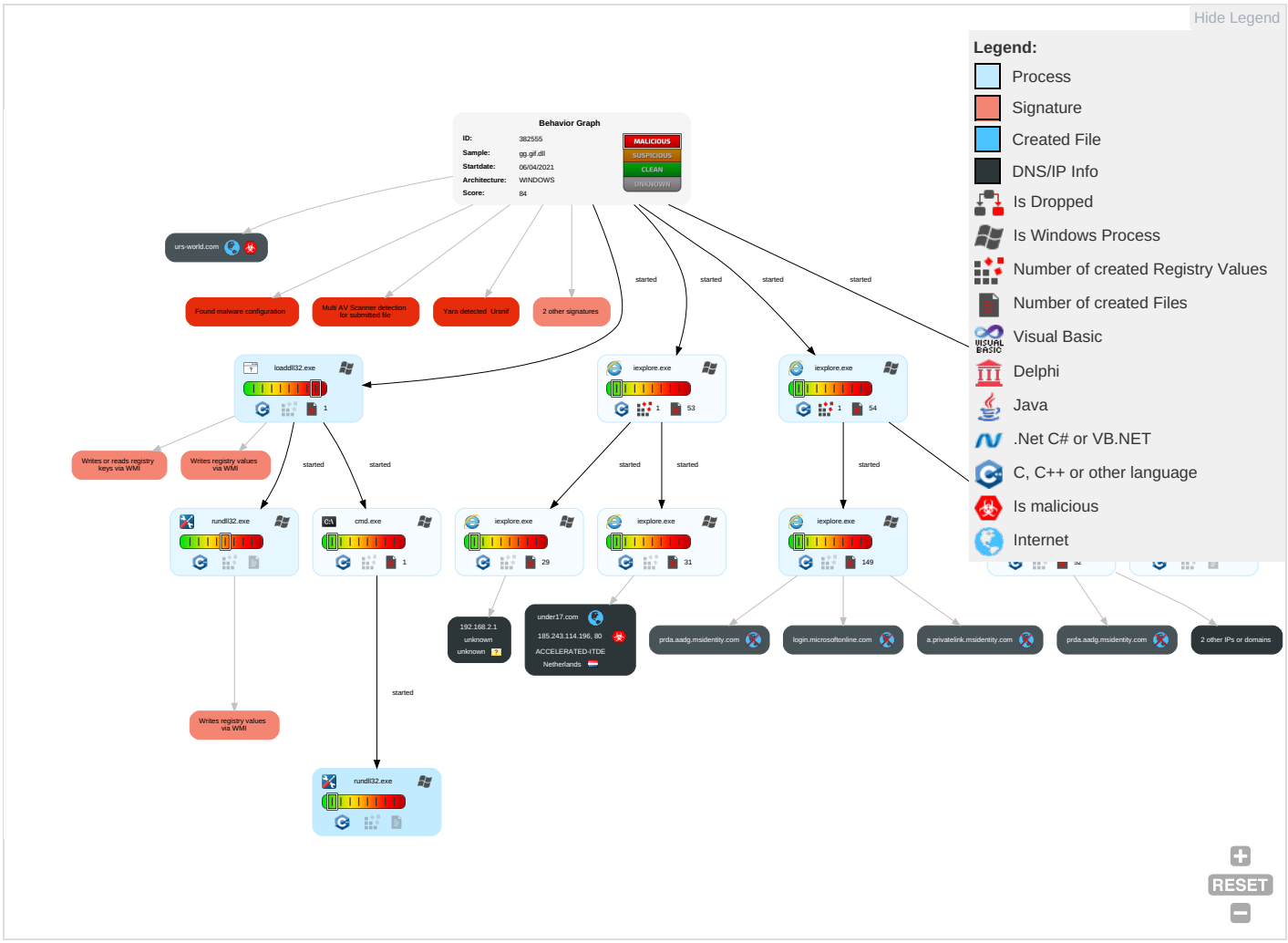
Yara detected Ursnif

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Rem Serv Effe
Valid Accounts	Windows Management Instrumentation 2	Path Interception	Process Injection 1 2	Masquerading 1	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	

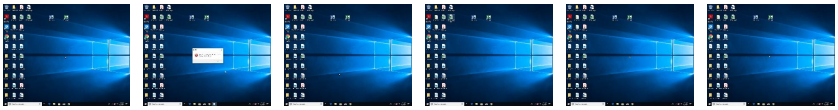
Behavior Graph



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
gg.gif.dll	52%	ReversingLabs	Win32.Trojan.Gozi	
gg.gif.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.47c0000.3.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.2ce0000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
0.2.loaddll32.exe.10000000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
3.2.rundll32.exe.10000000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://under17.com/joomla/b5_2FTUcdYX/sVnNArBfX_2BDo/zZv_2Fbn6M53QxtrfT64W/tg0Mz_2FW77FnY1h/4P95tKyS	0%	Avira URL Cloud	safe	
http://under17.com	0%	Avira URL Cloud	safe	
http://under17.com/joomla/qpONlUc_2Fx9bGWS/jLOColZsxiS4Q8t/VbkMaKiMRHZwpzblKX/6AI6KdKhU/1fj0ddZRJ_2F	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

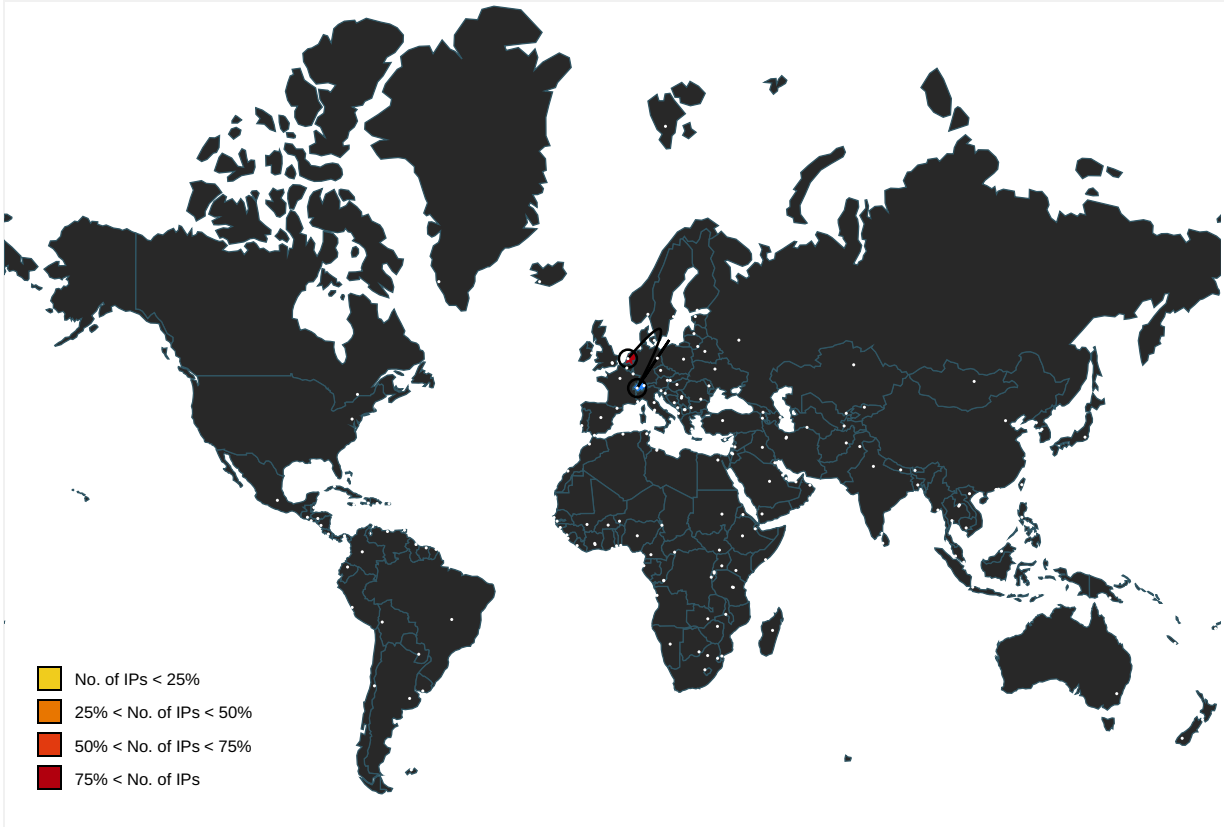
Name	IP	Active	Malicious	Antivirus Detection	Reputation
urs-world.com	185.186.244.95	true	true		unknown
under17.com	185.243.114.196	true	true		unknown
login.microsoftonline.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.msn.com/de-ch/nachrichten/politik/l	msnpopularnow[1].json.19.dr	false		high
http://https://www.msn.com/de-ch/news/other/das-grosse-impfen-beginnt-geht-es-nun-endlich-vorw	msnpopularnow[1].json.19.dr	false		high
http://https://www.msn.com/de-ch/finanzen/top-stories/janet-yellen-us-finanzministerin-fordert-weltweite-mi	msnpopularnow[1].json.19.dr	false		high
http://under17.com/joomla/b5_2FTUcdYX/sVnNArBfX_2BDo/zZv_2Fbn6M53QxtrfT64W/tg0Mz_2FW77FnY1h/4P95tKyS	{05FE9155-96AD-11EB-90EB-ECF4BBEA1588}.dat.25.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/de-ch/nachrichten/international/so-tickt-kosovos-neue-staatspr	msnpopularnow[1].json.19.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/international/es-h	msnpopularnow[1].json.19.dr	false		high
http://https://www.msn.com/de-ch/news/other/abdullah-sollte-von-erdogan-lernen/ar-BB1fktw7?ocid=BingHPC	msnpopularnow[1].json.19.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/vermischtes/die-altersheime-hat-man-vergessen/ar-BB1fkRPW?ocid	msnpopularnow[1].json.19.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/politik/das-alles-h	msnpopularnow[1].json.19.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/vermischtes/nachtleben-in-israel-eine-nacht-wie-fr	msnpopularnow[1].json.19.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/international/alexej-nawalny-klagt-	msnpopularnow[1].json.19.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/politik/manfred-weber-nennt-eu-beitritt-der-t	msnpopularnow[1].json.19.dr	false		high
http://under17.com	loaddll32.exe, 00000000.00000002.923372495.0000000001272000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/de-ch/nachrichten/politik/coronakrise-laschet-fordert-harten-br	msnpopularnow[1].json.19.dr	false		high
http://https://www.msn.com/de-ch/news/other/polizei-sucht-mit-superpuma-nach-vermissten-minderj	msnpopularnow[1].json.19.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/other/karl-lauterbach-der-blitzableiter-der-republik/ar-BB1fil	msnpopularnow[1].json.19.dr	false		high
http://https://www.msn.com/de-ch/finanzen/top-stories/staatliche-regulierung-allianz-gegen-big-tech-druck-a	msnpopularnow[1].json.19.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.msn.com/de-ch/nachrichten/politik/fdp-nur-keine-option-von-vornherein-ausschlie	msnpopularnow[1].json.19.dr	false		high
http://https://login.microsoftonline.com/common/oauth2/authorize?client_id=9ea1ad79-fdb6-4f9a-8bc3-2b70f96e	~DFF25467FE1B136D69.TMP.17.dr, {EA9F6200-96AC-11EB-90EB-ECF4BBEA1588}.dat.17.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/international/ukrainekonflikt-maas-warnt-russland-und-ukraine-	msnpopularnow[1].json.19.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/international/admirale-begehren-auf-gegen-das-verr	msnpopularnow[1].json.19.dr	false		high
http://https://www.msn.com/de-ch/news/other/ressourcen-f	msnpopularnow[1].json.19.dr	false		high
http://https://www.msn.com/de-ch/finanzen/top-stories/datenleck-bei-facebook-wachstum-z	msnpopularnow[1].json.19.dr	false		high
http://https://www.msn.com/de-ch/news/other/pentagon-usa-beobachten-russlands-aktivit	msnpopularnow[1].json.19.dr	false		high
http://feross.org	GiGr-rA9TBhE2c3LJn7PvDweiOo.gz[1].js.21.dr	false		high
http://under17.com/joomla/qpONlUc_2Fx9bGWS/jLOColZsxiS4Q8t/VbkMaKiMRHZwpzblKX/6AI6KdKhU/1fj0ddZRJ_2F	{05FE9153-96AD-11EB-90EB-ECF4BBEA1588}.dat.25.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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	382555
Start date:	06.04.2021
Start time:	09:50:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	gg.gif.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	32
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@20/112@8/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 57.7% (good quality ratio 54.5%) • Quality average: 78.8% • Quality standard deviation: 29.2%
HCA Information:	• Successful, ratio: 85% • 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): BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.113.196.254, 168.61.161.212, 92.122.145.220, 104.43.193.48, 20.50.102.62, 92.122.213.194, 92.122.213.247, 88.221.62.148, 52.155.217.156, 13.107.21.200, 204.79.197.200, 131.253.33.200, 13.107.22.200, 20.190.154.17, 40.126.26.134, 40.126.26.135, 20.190.154.137, 40.126.26.132, 20.190.154.139, 20.190.154.18, 20.190.154.16, 40.126.31.136, 40.126.31.9, 40.126.31.7, 20.190.159.131, 40.126.31.5, 40.126.31.2, 20.190.159.135, 40.126.31.140, 40.126.31.8, 20.190.159.134, 20.190.159.138, 40.126.31.141, 40.126.31.4, 40.126.31.137, 20.190.159.132, 40.126.31.1, 2.20.142.210, 2.20.142.209, 20.54.26.129, 40.88.32.150, 152.199.19.161 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, store-images.s-microsoft.com-c.edgekey.net, bing.com, a1449.dscg2.akamai.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, e11290.dspg.akamaiedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, iecvlist.microsoft.com, teams-9999.teams-msedge.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, login.live.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, www2.bing.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ie9comview.vo.msecnd.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, www.tm.a.prd.aadg.akadns.net, a767.dscg3.akamai.net, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, wst.current.a.prd.aadg.trafficmanager.net, www2-bing-com.dual-a-0001.a-msedge.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, teams-ring.teams-9999.teams-msedge.net, teams-ring.msedge.net, displaycatalog-rp.md.mp.microsoft.com.akadns.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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/382555/sample/gg.gif.dll

Simulations

Behavior and APIs

Time	Type	Description
09:51:22	API Interceptor	1x Sleep call for process: rundll32.exe modified
09:51:22	API Interceptor	1x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.243.114.196	gg_1.gif.dll	Get hash	malicious	Browse	
	gg_2.gif.dll	Get hash	malicious	Browse	
	KcFVz0y2si.dll	Get hash	malicious	Browse	
	bTjvWUTLid.dll	Get hash	malicious	Browse	
	KAsJ2r4XYY.dll	Get hash	malicious	Browse	
	swlsGbeQwT.dll	Get hash	malicious	Browse	
	document-1048628209.xls	Get hash	malicious	Browse	
	document-1771131239.xls	Get hash	malicious	Browse	
	document-1370071295.xls	Get hash	malicious	Browse	
	document-69564892.xls	Get hash	malicious	Browse	
	document-1320073816.xls	Get hash	malicious	Browse	
	document-184653858.xls	Get hash	malicious	Browse	
	document-1729033050.xls	Get hash	malicious	Browse	
	document-540475316.xls	Get hash	malicious	Browse	
	document-1456634656.xls	Get hash	malicious	Browse	
	document-1376447212.xls	Get hash	malicious	Browse	
	document-1813856412.xls	Get hash	malicious	Browse	
	document-1776123548.xls	Get hash	malicious	Browse	
	document-684762271.xls	Get hash	malicious	Browse	
	document-1590815978.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
urs-world.com	gg_1.gif.dll	Get hash	malicious	Browse	• 185.186.244.95
	gg_2.gif.dll	Get hash	malicious	Browse	• 185.186.244.95
	bTjvWUTLid.dll	Get hash	malicious	Browse	• 185.186.244.95
	KAsJ2r4XYY.dll	Get hash	malicious	Browse	• 185.186.244.95
	swlsGbeQwT.dll	Get hash	malicious	Browse	• 185.186.244.95
	document-1048628209.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1771131239.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-69564892.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1729033050.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1813856412.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1776123548.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-647734423.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1579869720.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-895003104.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-779106205.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-806281169.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-839860086.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1061603179.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-909428158.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1747349663.xls	Get hash	malicious	Browse	• 185.186.244.95
under17.com	gg_1.gif.dll	Get hash	malicious	Browse	• 185.243.114.196
	gg_2.gif.dll	Get hash	malicious	Browse	• 185.243.114.196
	KcFVz0y2si.dll	Get hash	malicious	Browse	• 185.243.114.196
	bTjvWUTLid.dll	Get hash	malicious	Browse	• 185.243.114.196
	KAsJ2r4XYY.dll	Get hash	malicious	Browse	• 185.243.114.196
	swlsGbeQwT.dll	Get hash	malicious	Browse	• 185.243.114.196
	document-1048628209.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1771131239.xls	Get hash	malicious	Browse	• 185.243.114.196

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ACCELERATED-ITDE	gg_1.gif.dll	Get hash	malicious	Browse	• 185.243.114.196
	gg_2.gif.dll	Get hash	malicious	Browse	• 185.243.114.196
	KcFVz0y2si.dll	Get hash	malicious	Browse	• 185.243.114.196
	bTjvWUTLid.dll	Get hash	malicious	Browse	• 185.243.114.196
	BnJvVt951o.exe	Get hash	malicious	Browse	• 152.89.236.214
	BnJvVt951o.exe	Get hash	malicious	Browse	• 152.89.236.214
	SMtbg7yHyR.exe	Get hash	malicious	Browse	• 152.89.236.214
	KAsJ2r4XYY.dll	Get hash	malicious	Browse	• 185.243.114.196
	swlsGbeQwT.dll	Get hash	malicious	Browse	• 185.243.114.196
	document-1048628209.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1771131239.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1370071295.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-69564892.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1320073816.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-184653858.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1729033050.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-540475316.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1456634656.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1376447212.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1813856412.xls	Get hash	malicious	Browse	• 185.243.114.196

JA3 Fingerprints

No context

Dropped Files

No context
No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{05FE9151-96AD-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	50344
Entropy (8bit):	1.9969942287314704
Encrypted:	false
SSDEEP:	192:rcZfZx2uWIt+ife20zMy8B28DWFFcfbvAuMOhvAvFvwfnlvwtkbCewm3bGe+FNuC:rchAFsvDXZUIa/YQ
MD5:	DFE3D02A1579698EFF82C1C921B68CBB
SHA1:	F1FE7E02D0F8A84A025F1EC6EB9E531BCB1DBE43
SHA-256:	04EA7F40D60CB440CBA0BF166970741CD0EA1318893D50E2B9F439307A6C5D8A
SHA-512:	56E08C4D4EF80B0B035D15803E0CE18F73F9927F9A66B5F8264742F283D6646E7496F6BC1980026121587C47DEA1DC2C5A08C12BD12D81DAE73840B3917CAFAE
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{1C24251B-96AD-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	12888
Entropy (8bit):	1.5862929781759378
Encrypted:	false
SSDEEP:	48:IwijGcpr2wGwpLIpG/ap8c6iGIpccAeGvnZpb:rqZ9ZO2cHWcYB
MD5:	A13D1E98A2EE092964B0C8E1F46B05B6
SHA1:	FCCE3972D2212D6248391D76A1C936AC68548ADB
SHA-256:	3076019DA18EFC38D82647A0E6A1979A43543B0ECB12C282C5B3E11652A49232
SHA-512:	BAA3BBFED699EA957E1E6A5C1C01308F35484317200D24EA7F380F9372E8A37F0476558F15A1E1CC1B9D34FD269CB158258BD79E613BE5F26F25F270C401FFA8
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{EA9F61FE-96AC-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	50344
Entropy (8bit):	1.9933650725731136
Encrypted:	false
SSDEEP:	192:rGZ5ZD28WytYifShPzMLHB4HDMKsc2wC5uMkWC5awC7tMIDC7tVwwb7w3wKbLZvt:rCv6rKFjdGC0LVqJ
MD5:	5151377191C42A6C52FF24C9E2FB5C16
SHA1:	9A437E47213BEC4FD05E8709921BC7A214BAD703
SHA-256:	8A0AC5BFB9EE34B3AA83D1DC59187E84326CDFD654DE81F52BA844D9FB293AF4
SHA-512:	A27D1577C532345921E8C0B64878E7682AAE374946E6726EDC7BE5AB19BCDCB979198B3A0CF68E597B0BDD71BEAC3A1E0E203853577B0216AC2BE40966F470F9
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{05FE9153-96AD-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27364

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{05FE9153-96AD-11EB-90EB-ECF4BBEA1588}.dat	
Entropy (8bit):	1.8429941639135412
Encrypted:	false
SSDEEP:	96:r/XZMQYz6aBSgj52VWeMeGiZsyVRiZsyo/QA:rPZMQc6akgj52VWeMeGPyVRPyhA
MD5:	C32E80CE56AB9E15F368FC84EDB57149
SHA1:	001C1F5F09720FBDC171CB67B01C4544DFDB5F44
SHA-256:	2827586B32B665B517471318195255C879E7FD09D9817D646349D3061477CA9C
SHA-512:	5D81DE40BEE7F167764BC33944DB71F3D3B8BFEB0FC8AAB437CFFF962AB3C0FBDD1DB450BC06961C50D357264A6ABC06530A3DF6D547E1C8A43C5C29544D4B3
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{05FE9155-96AD-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	27864
Entropy (8bit):	1.8290028415875113
Encrypted:	false
SSDEEP:	48:Iw/jGcpraGwpaOjG4pQWGrapbSciGQpBVsGHHpcVxTGUp8V5GzYpmVf5GopQHfV1:rhZCQ66YBS1jF2xWdMRS9JIYR9Jlx8r
MD5:	7B79A17C2F3B85B5B34315866D761CD7
SHA1:	976C39DF1A616EE5BC3B6145C9E6ED98A186CE3E
SHA-256:	7539999D838FA1A81D3A9BE73FAFA95B82983592B8B272DB1BD4B64553D79A7C
SHA-512:	9DA226A0F1E1A83CBCC5BFC7F5F7DF964C035C292F59D84F2CAB62B032343A4E01DE2010A352D99BD457D04FCD073237B37E4B9AB96D796B3F788B059FFEC08
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1C24251D-96AD-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	5720
Entropy (8bit):	1.4340406914706598
Encrypted:	false
SSDEEP:	12:hmFQCb77ll3l09lCgQF4jrEgm8Gz7qDplRI9l26auFXrEgm8GL7apl0Ym4:I49lLXjG8NpQ9lImG8xpR
MD5:	CA23C743BF84FB5B655CC515FB1549A1
SHA1:	69124FE788875A971E81303733DC33F577329161
SHA-256:	DB94BEF9FB0D7743E30CE5269393284D3E1A5692C2333E80B3F28E36AEA03AC3
SHA-512:	81800A66219E76B6EBC01CAD70F958C32EA9DB39F6637ED4A7E4F7922C78873E3CE43520BBD6B27D78478326B3BFE2F5B73011D03DF71DF32F2EA638EAED8C84
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{EA9F6200-96AC-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	43196
Entropy (8bit):	2.499623083906951
Encrypted:	false
SSDEEP:	384:rXT2OIwY3hNPPyCI50fGa/fGasUfGalp5ktMXi:GznzLz/i
MD5:	14951CC9835396D3DD4302BCE50242A3
SHA1:	4788B9CC4F818DA564E07DC2AFBECEEC36CDC671
SHA-256:	A823174998CA2F2FE8AB198D30B94EA8140CCB236D5512F7A137438FB7F80E5B
SHA-512:	52FC8029D16F98B3EA487B6F17AC31A78BF4D089D7E103B49661483BB84BEC97FD6D4A37D41E51BC1F679C052A65987920756DC57093D26C36674F4E7884F361
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{EA9F6200-96AC-11EB-90EB-ECF4BBEA1588}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{EA9F6202-96AC-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	43196
Entropy (8bit):	2.5015573481732405
Encrypted:	false
SSDEEP:	384:rmKUUiAUomnuPyCI50fn2Cfn2VUfn2gOT9zKH:5n2En2En2g
MD5:	EB8CA53B544C1868AD15C58F6EAFAF0A
SHA1:	753A7DFCA49528B53D0A3FB2690047F2931D1A22
SHA-256:	05F91C1D2C6F67AC017AC969658BC10FDF9DC9D8F7E20C1DE57D3DE7C7DA006D
SHA-512:	42BE0DBB6E5873FFE474F1F62ABEA40E258039717FEBF4FB4940D7A0650A3BFB6655638060D966A837DEEC9F04665E54DCCF4BA6C355211B1B0555B8163380D
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	10192
Entropy (8bit):	4.534930299499423
Encrypted:	false
SSDEEP:	96:0Ph+Qhato4xfDehrmrPh+Qhato4xfDehrm+:0Z+dnxDehKrZ+dnxDehK+
MD5:	1AABD44CA697BF3C91EF3CB3A8EF1600
SHA1:	B17D34A8C67CECB4C7B3651C44E0A369D1FD6C1A
SHA-256:	F0F3C4D9EC8DE0CA03E76823CC6408BAB62BA4253D738542F89ECC81B1D985EC
SHA-512:	7C994D1F7EE87026BBEE660FEC637D7600B202FA51A4DC017E3E5C0D7FD67487FFF36CDD51650078066580C1124654D06B24A339ACCE158E8C74A50C8FC26C
Malicious:	false
Preview:	+.h.t.t.p.s.:././.w.w.w...b.i.n.g...c.o.m./.s.a./.s.i.m.g./.f.a.v.i.c.o.n.-.2.x...i.c.o..... ....(... ...@..... .....N...Sz..R...R...P...N..L..H..DG.....R6..U...U...S...R...P...N..L..I..F. .B...7.....S6..V...V...U...S...R...P...N..L..I..F..C...?..:z.....O...W...V...V...U...S...R. ..P...N..L..I..E..C...?...;..{7..q2$.....T..D..]...S)..p6..J...R...P...N..L..I..E..B..>..;..z7..p2..f,X.....A..O#..N!..N! ..N!..P$..q:...P...N..K..I..E..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\BJp5dDFvoQm12CHBfp4PC6aiyg4.gz[1].css	
Category:	downloaded
Size (bytes):	73202
Entropy (8bit):	5.307816444057117
Encrypted:	false
SSDEEP:	1536:kcGJTL/mKzAAFl7JlsG0GRe1cxnoWC1kuyOYkTs/Kun:LGJ4AFl7JlsG0GRCcxnoWC1kuyOYkT0
MD5:	C912DA2683E71660357A600EE34A7873
SHA1:	5DFD028307D4CD8A66492E807B848FEC177AEC3A
SHA-256:	525D57B5D38D8212993C66A33F4CD15EDBD0F260A5AFCF539D092047A908D6EE
SHA-512:	31E2A56C27CC037AD903292DFA518E86642C2A610E9923DD4F7A2FD1347167E042E957A85E98561CC9178318D121DEA3EF165F88EEC79915D0687939DC25BBC
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/BJp5dDFvoQm12CHBfp4PC6aiyg4.gz.css
Preview:	.scopes{color:rgba(255,255,255,.8);display:inline-block;left:0;white-space:nowrap;list-style:none;line-height:39px}.scopes.sc_hide{display:none}.scopes .scope{font-size:.8125rem;cursor:pointer;vertical-align:middle;margin-right:36px;background-repeat:no-repeat;position:relative;display:inline-block}.scopes .scope:hover,.scopes .scope.focusin{color:#fff}.scopes .scope:hover .overflow_menu,.scopes .scope.focusin .overflow_menu{transform:none}.scopes .scope:focus-within .overflow_menu{color:#fff;transform:none}.scopes .scope a{color:inherit;cursor:pointer;text-decoration:none}.scopes .scope.dots{margin-bottom:8px;font-weight:bold}.scopes .scope.dots:before{display:inline-block;content:'. . .'}.scopes .scope.dots.hover_focus:focus{outline:none}.scopes .scope .overflow_menu{color:#666;cursor:pointer;transform:scale(0);position:absolute;background-color:#fff;border-radius:6px;padding:4px 0;box-shadow:0 4px 12px 1px rgba(0,0,0,.14);min-width:155px}.scopes .scope .overflow_menu .overflow_item{

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\JDHEvZVDnqsG9UcxzgIdtGb6thw.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	408
Entropy (8bit):	5.040387533075148
Encrypted:	false
SSDEEP:	12:2QWV6yRZ1nkDXAn357CXYX0cO2mAICL2b3TRn:2QO6P+5OYXJPi3TRn
MD5:	B4D53E840DB74C55CC3E3E6B44C3DAC1
SHA1:	89616D8595CF2D26B581287239AFB62655426315
SHA-256:	622B88D7D03DDACC92B81FE80A30B3D5A04072268BF9473BB29621E884AAB5F6
SHA-512:	4798E4E1E907EAE161E67B9BAB42206CE0F22530871EEC63582161E29DD00D2D7034E7D12CB3FE56FFF673BC9BB01F0646F9CA5DAED288134CB25978EFBBECF
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/JDHEvZVDnqsG9UcxzgIdtGb6thw.gz.js
Preview:	(function(){function u(){n&&(n.value.length>0?Lib.CssClass.add(sj_b,t):Lib.CssClass.remove(sj_b,t))}function f(r){n.value="";Lib.CssClass.remove(sj_b,t);sj_log("CI.XButton","Clicked","1");i&&Lib.CssClass.add(i,"b_focus");n.focus();n.click();r&&(r.preventDefault(),r.stopPropagation())}var i=_ge("b_header"),n=_ge("sb_form_q"),r=_ge("sb_clt"),t="b_sbText";n&&r&&(sj_be(r,"click",f),sj_be(n,"keyup",u),u())})()

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\NnFHhz2jL6yzChtIhaB5IIVKY5k[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1111
Entropy (8bit):	4.61511796141903
Encrypted:	false
SSDEEP:	24:twgonGLheJUVYxCdBTMqTS05sLGkkhQgbQgwHW4QhJ:6gAShpyxCdBTrS05sLKhvUfSJ
MD5:	C04C8834AC91802186E6CE677AE4A89D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\NnFHhz2jL6yzChtIhaB5IIVKY5k[1].svg	
SHA1:	367147873DA32FACB30A1B4885A07920854A6399
SHA-256:	46CC84BA382B065045DB005E895414686F2E76B64AF854F5AD1AC0DF020C3BDB
SHA-512:	82388309085BD143E32981FE4C79604DCEFC4222FB2B53A8625852C3572BDE3D3A578DD558478E6A18F7863CC4EC19DFBA3EE78AD8A4CC71917BFFE027DC22 0
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/NnFHhz2jL6yzChtIhaB5IIVKY5k.svg
Preview:	<svg width="20px" height="16px" viewBox="0 0 20 16" focusable="false" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">.. <g transform="translate(-10, -12)" fill="#007DAA" >.. <path d="M28.125,14.4615385 L25,14.4615385 L24.26875,13.0203077 C23.95125,12.3950769 23.30125,12 22.59125,12 L17.40875,12 C16.69875,12 16.04875,12.3950769 15.73125,13.0203077 L15,14.4615385 L11.875,14.4615385 C10.84,14.4615385 10,15.2886154 10 ,16.3076923 L10,26.1538462 C10,27.1729231 10.84,28 11.875,28 L28.125,28 C29.16,28 30,27.1729231 30,26.1538462 L30,16.3076923 C30,15.2886154 29.16,14.4 615385 28.125,14.4615385 Z M20,25.5384615 C17.23875,25.5384615 15,23.3341538 15,20.6153846 C15,17.8966154 17.23875,15.6923077 20,15.6923077 C22.76125, 15.6923077 25,17.8966154 25,20.6153846 C25,23.3341538 22.76125,25.5384615 20,25.5384615 Z M20,18.1538462 C18.62125,18.1538462 17.5,19.2578462 17.5,20. 6153846 C17.5,21.9729231 18.62125,23.0769231 20,23.0769231 C21.37875,23.0769231

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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+lvyUJ9sq5aOB: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=["shdl gapi",n],i=0;i<t.length;i++)r.push(t[i]);sj_evt.fire.apply(null,r)}n.bootstrap=i;n.show=r;n.showError=u})(ShareDialog||(ShareDialog={})),function(n){function i(){t==0&&u( )}function r(){sj_evt.unbind("shdlgapi",i)}function u(){t=1;var n=ShareDialogConfig.shareDialogUrl+"&IG="+_G.IG;n=e(n,["uncrunched","testhooks"]);sj_ajax(n,{callback:func tion(n,i){n?(t=2,i.appendTo(_d.body),r(),f()):t=3},timeout:0})}function f(){var n="rms";_w[n]&_w[n].start()}function e(n,t){var i,r,u;for(r in t)u=new RegExp("[?&]"+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\2WF3MMUU\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.querySel ectorAll(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.en queue(t,e)}}var t="L";n.wireup(t,{load:null,compute:i,unload:null})})(BM)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493 AC6D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\dnserror[1]	
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\2WF3MMUU\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\favicon-2x[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 32x32, 32 bits/pixel
Category:	downloaded
Size (bytes):	4286
Entropy (8bit):	3.8046022951415335
Encrypted:	false
SSDEEP:	24:suZOWcCXPRS4QAUs/KBy3TYI42Apvl6wheXpktCH2Yn4KgISQggggFpz1k9PAYHu:HBRh+sCBykteatiBn4KWi1+Ne
MD5:	DA597791BE3B6E732F0BC8B20E38EE62
SHA1:	1125C45D285C360542027D7554A5C442288974DE
SHA-256:	5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07
SHA-512:	D8DC8358727590A1ED74DC70356AEDC0499552C2DC0CD4F7A01853DD85CEB3AEAD5FBDC7C75D7DA36DB6AF2448CE5ABDFF64CEBDCA3533ECAD953C061A9338E
Malicious:	false
IE Cache URL:	http://https://www.bing.com/sa/simg/favicon-2x.ico
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\2WF3MMUU\fdVZU4ttbw8NDRm6H3I5BW3_vCo[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	671
Entropy (8bit):	5.014579690661168
Encrypted:	false
SSDEEP:	12:tbH4/KYf3UnlcWYl7qy/gk63xsV8tGXcqecDDWUV8jEPsycd23Wt+MKsAnueOc+d:t74LfEnTYpq+gTxs6GUUQEPssmYsAnuH
MD5:	D9ED1A42342F37695571419070F8E818
SHA1:	7DD559538B6D6F0F0D0D19BA1F7239056DFFBC2A
SHA-256:	0C1E2169110DD2B16F43A9BC2621B78CC55423D769B0716EDAA24F95E8C2E9FE
SHA-512:	67F0BC641D78D5C12671FDD418D541F70517C3CA72C7B4682E7CAC80ABE6730A60D7C3C9778095AAB02C1BA43C8DD4038F48A1A17DA6A5E6C5189B30CA19A15
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/fdVZU4ttbw8NDRm6H3I5BW3_vCo.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\fdVZU4ttbw8NDRm6H3l5BW3_vCo[1].svg	
Preview:	<svg focusable="false" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 16 16" enable-background="new 0 0 16 16" xml:space="preserve">..<path fill="#919191" d="M15.707,0.293c-0.391-0.391-1.024-0.391-1.415,0L7.994,6.591L1.696,0.293C1.298-0.091,0.665-0.08,0.281,0.318...c-0.375,0.388-0.375,1.003,0,1.391l6.298,6.298l-6.298,6.298c-0.384,0.398-0.373,1.031,0.025,1.415c0.388,0.375,1.003,0.375,1.391,0...l6.298-6.298l6.298,6.298c0.398,0.384,1.031,0.373,1.415-0.025c0.375-0.388,0.375-1.003,0-1.39L9.409,8.006l6.298-6.298...C16.098,1.317,16.098,0.684,15.707,0.293z"/>..<path fill="none" d="M0,0h16v16H0V0z"/>..</svg>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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:	E7F2603855A16464417B772517676F080CCEFFB8069C687BAC798B7EB2875FCDC207E40E8C56E7CFFD4D56CED572270988599D1D2B73FB8AAA7FDD076FE3E7E7
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/hceflue5sqxkKta9dP3R-IFtPuY.gz.js
Preview:	(function(n){function i(){var i=document.documentElement,r=document.body,u="innerWidth"in window?window.innerWidth:i.clientWidth,f="innerHeight"in window?window.innerHeight:i.clientHeight,e=window.pageXOffset||i.scrollLeft,o=window.pageYOffset||i.scrollTop,s=document.visibilityState||"default";n.enqueue(t,{x:e,y:o,w:u,h:f,dw:r.clientWidth,dh:r.clientHeight,v:s})}var t="V";n.wireup(t,{load:null,compute:i,unload:null})})(BM)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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:	D52D1CCBBEDDC49B850030E3B2ABA9EADE824AE74EF4FF7055D50EDDCABC7933D6D662FEE8DF0F37B20F096E96908DA0CB89FF8DFC4E6AB14F1255BBDE745A40
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\2WF3MMUU\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:	D61045D1F07ED241626B8233D388F5E1AD54DBE224871E1CE872ECFD0E29F05A21F0EA02FFDE688FACB134DD969533615493BD35EBA4D5E755840C30A687EE0
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\2WF3MMUU\th[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	3726
Entropy (8bit):	7.864083694829938
Encrypted:	false
SSDEEP:	48:pyYcuERAB4Zyb8BrwdM18WIaMAVwIIjMC+FrFza8JmQOQYBhvSp/BSq/DVimjw:pPEZc8ROMWWLMcj7rFza8/VY4MsVij
MD5:	A6E6FD3AB66E5A2F49A45CCB2B61B19D
SHA1:	9A7EC1C26991AFC76B694BECB95639DDE2AB9DA2
SHA-256:	8FB3DE41169B7B8547E4F07836C9C9503655B613678E58DE449A0CB65DFACCE4
SHA-512:	278DD1A867D863F595FB3B8398399F5EAFC332FB29981EF4BF9B14DBCBFBC55A9AC2CE3A86EB4A95F6CFC8C8BE9B60FF690BF9AB436D2AD270A3981ED23B47B
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkXNm.img&ehk=kxyU8xKPJMs4tMRWRT6cTgj6Bfiij4nG3t8YLJw8HCQ%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....``.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)===.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....i....Q..@...P.c....8..;..*..\.@.>.....+.:iV.c.0.D.ub.j._..7.G....f.$(..p2....MsN..b..3+tBy>.Z.O.h. .e.O..e....n +._g....p.{....x.f..o,<^...g.\>....7P.*R..#..b0kB..%%tq.....Q@..Q@...u!...(...R.v(..KE.....{....H'.....U,!X.2....K.sa2...p.W8..s...GL...Q./0v.2..$q...q..Gv.....!.r...IU..._U....AYZFn.H^=I=.e..B.+\l4..I.y..p@...j.....A...M.+.v:lG.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\th[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	3792
Entropy (8bit):	7.879458150606813
Encrypted:	false
SSDEEP:	96:pPEUZavUpaPPjl0qwzhf5Q6u2i7HGLHFgak2bB+u+iiKaCPg8o:pPH0vUWlqhf5Q6uZiDFgak3neaFF
MD5:	E5D2688116BA8D4ABBC53F2493A181BE
SHA1:	2330F5A38AB1DE6979790C84B33DC173F853D6FD
SHA-256:	AA1EF9A296A78952F642406AA0F59930CDD23BC5D1714B7E306787CD4064229E
SHA-512:	0FEBAA0286AFF016B5F0B2B9984D95E2319CA29E41AF624A50D5BF1EDA33CD61017226312DE65B1E5A169A95DB7A6F9212EFFC06A498B0BA857C744CCCBDE3BA
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1flaPv.img&ehk=nfyoU%2b8cc2O%2frjxfHaxiAbz0t%2fXYbGhU6jS%2bwZAdcS0%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....``.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)===.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..x.[.G....uz.....M8.....4..l..2..?..9....$q..r./...LE...'o...w.[H.J..Z..G..Nl.....gC..pk.n..hF.+..<..V...d).....,.Bpj.DT...Rl-..@...i..L.....e.*&(..`...P...l..J.....@.Mqc}z.....>..)U,y.^.Aq...X...QG.8W....Q..]^..j.|.n~X...[.....\.n.i0..#..9..<Wk.....bx.._.....idb3.A..k7+.....,.M./..@...2.?.Y}M....$.....)=....w]....>Y..t+.I....Z.9$.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\th[3].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\th[3].jpg	
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 144x144, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	4662
Entropy (8bit):	7.906652539569635
Encrypted:	false
SSDEEP:	96:pPE9fuJsPbx60IPg+MMuPecZoXnNRLW/wG+fWRY:pPaf7bx6rg+7XnNRnGRY
MD5:	49A2DFF8082FCF50F4311C7867ECEDAD
SHA1:	A125B14C82BFB9A78C711C13CC479FDD1C9266EA
SHA-256:	442192ACEE743DBF8DBEC6A3BA8212AF4FDCFA1E08E96894168F11011176F525
SHA-512:	088A01E123048CB37238D611B7F01218EEDDF846FF42875AEDB756D91819B06A131ED272067E66C76C538112C14F676213D6EC5EA4B0D353B68E7BE056F0F08A
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkzlb.img&ehk=VW7SkyKxbL7LXUGh4v%2fSqtV2Ju%2b%2fdtlvyipIBuf1oQo%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=========.. .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....4..@.j.=AA9$....M..R.1..&...M#....:.C..@..?.!.=i.A.j..-.....*.`..".".sH.)s.Oj.z...T.O4...N.....wz.6.....=.....@.....E .(.P.w.M'&.z.Zg.4.....Tc.g.L..ny. (.i.....C[..e.G...7{..Y.Ff.P...}.vvL..G....K.6.,.....a@..jve. .#"...c.m.8.X{.T..b..9....+..4X%?....Eq.v..N.L.#.....P.T..<W/.L...>e9..{..ja<.j3..,Py.. ...h.t..J8...~R=...i..v.0.4Ss..RP ..iI.R..9{.S..j^.CG

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\th[4].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	5639
Entropy (8bit):	7.924649163999842
Encrypted:	false
SSDEEP:	96:pPECr5OAvlqY/K2/QGjfn7l0xXDUduR+Ksxd18Up0FlXDmR6vhOjUEbDdl:pPnOAvlh/KXGf7LxXDUd2kd6XbbOgEbT
MD5:	CB467408920B249304F096825FAD3555
SHA1:	34B1FB66BB1993D6F421D03E60571B2D6B8BD82B
SHA-256:	6244F0B65FD5FDB55035289E22AE746FDA4FB8A73FA5099AC1765FE40EBF15F3
SHA-512:	66499CCD7720806D8D469F36F1BA68B8654C4113F6EC8952C30B0B7A5456CE7B942E535389026532315054070O3DF5D6EC55402114F39FEB6EE135B6B803BC60
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fk8uF.img&ehk=3yVhb5eiLjVCrnzpfMt8vNf6P4rYdQzaUR6b8msklWU%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....,.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=========.. .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....I.5Zo1..{V}.W..3.w...@..>..^...8I.U..b..k.....<..1J".[..>..."f...`.U...$V..C...ZfzF...V.R...-....r=G4.....LD....[.D\..*....w.h..R1&..z...'.1.#..i.w..{P H*p.@/..B..&..9..{]].0..{.RT....>.....0.Y.Q...3[).....q.....>.}OX...Y..:....r.@k.@..Fy0.<....i.j.....t.9\gp..j.v...~.+..#...&q.5zH.JYW.cry.,....9o.3..r...G .z..j.'..{X.-t..(S8.;...Q....N.<...._....'. .Z.:.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\th[5].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	6321
Entropy (8bit):	7.930428341817175
Encrypted:	false
SSDEEP:	96:pPEFWBYC3qBZJigkG/FdQS5zwu3LHBaWc4TUpz35BH7zQx5+FixuTKn7xF:pPGYYCaHsSdQSy8LHBaV4TU15tnQub2F
MD5:	AFF39E85868825504E8463C5CDD11BD7
SHA1:	DEF891B9A50BA0F8DA20DC93D5DFD80FFE330478
SHA-256:	17C3E9E4228BCBF6E56795D6D8539791483D4B1A07E4A542F32282D99C94FB75
SHA-512:	019D7C4382FEEC7EA3E7E26C20620327A9644A10AA13AEA9161C70DB8AAAD22BE452D4AF3D25E2C153C875BBA7D7C4B68D1EB2E128A212FB3E95C1F2568D9E B7
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkGZS.img&ehk=QmtuVlo%2bL0J6PRmZTHf5eMhHSpsWN3gSG5N88RqgPWU%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....,.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=========.. .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..4.._.]...O..X...k...^=.D.....k.m.H..$....C.kP[I,%.K.....G\....x..v....B.....?..uT....K.q.Kn".YV01.x.3A..O.I.a:.....R.!.#.e..YSqv{y....=y^...f.... ..W.Yx...!.d.....+..\....h.....S.L../X{.2..V...^.*q../Q[...f.....)...m..z..#.d.....v.~&.....#.V..A..z..W.i..O.B.HF2Y....T. ..FO..7....*G...xJ....r}.....;....';..P..N.G.R?..T.fq.....x

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\th[6].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\th[6].jpg	
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	5109
Entropy (8bit):	7.913384769447657
Encrypted:	false
SSDEEP:	96:pPELkaw+eKa2pvAJqZbK+VEYjHOxNtlurSUmBjQFr5i8T:pP0kaw+eKXfG+VEYyx1eSUmBI5/T
MD5:	27368154F2C3CF4EDEBC0A95CED35B43
SHA1:	5CAE3ECA10C9A32BC77AF7AEE1E2944590B8BD37
SHA-256:	4406423DC5F852B966777DE5272126839793C96251AB2F063A099C347BE396D9
SHA-512:	8313894648ADD4EF180464FA901403AB911B67A256DE09ACA665D66BA9EAEAE62A67624C3985F3E22BE537E4E8764FD32BD85C06BE7C3CD37A2418FDAD963E(C
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fk2g2.img&ehk=6LEOa661FEfcyTEYPdN22SbtYfGFBqG3UnhDMs6fDjo%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....`.`.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=========.. .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...<V>.....I..y5..t.z.K.Z.o.8.Y....]N.e"^Jv....:.+..$K..m..v.}..v./0R._j.....w.?...=.0.g.E>`..>...P>.Gc]..3.mb=.....Jq..M.H=k.k..B.dg.8.N.....3o .]..*z. P..?.O.9N(...M7i...}..v.}...|..9z+.}.....b;Q..cQZm.7....X...X.....1.c..IIK..k...b3.k.x..N{5q..|.\.:1.5Y.eQ..\.'...&..~.O+..9u.{…a].....|:.8Z,3.....C..I.....[z..V.-...Q.....x.....Y.g..q....mN.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\ELqKWpA6KkapLUFbOLS-IQ2zfXc[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=5, xresolution=74, yresolution=82, resolutionunit=2, software=GIMP 2.10.8, datetime=2019:08:01 11:43:45], progressive, precision 8, 160x160, frames 3
Category:	downloaded
Size (bytes):	9908
Entropy (8bit):	7.8062296698930025
Encrypted:	false
SSDEEP:	192:sWK8UVOGWSkbr43J1ZBpYKL2wth0XM2Cc8AyJKl4xV0KamWtOb+SP0cX:s18bVBrK9B6G2whJ2i/cmygrP0e
MD5:	968C49AC8A1A3EF85F2884F226C55742
SHA1:	10BA8A5A903A2A46A92D415B38B4BE210DB37D77
SHA-256:	E441AFC03F067D1D85DF1F69EB8F482BFDA697CC217E11E1547B3CE964B15B2A
SHA-512:	07B13D6E736683E36091E5BC52F953F9077AD9CD656F0F91E52F17C4630BE3D7524000AA37CFD6CB29ECBB5315F973086630F240118DBE248B4F8A3E79B2B524
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/ELqKWpA6KkapLUFbOLS-IQ2zfXc.jpg
Preview:	......JFIF.....H.H.....PExif..II*.....J.....R...(.....1.....Z...2.....f...z...H.....H.....GIMP 2.10.8.2019:08:01 11:43:45..... .....a.....JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222 22222222.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...M.....*.i.@.=h.....)(.....)i(....(.h...)h...ZJZ.(...(...(....(...)i(.....M.N4...S..4..!.E.....(.....(...Z(..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\H_VmuFPRwWZ4UrVl0mPztnf3z5U[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=5, xresolution=74, yresolution=82, resolutionunit=2, software=GIMP 2.10.8, datetime=2019:08:01 11:38:22], progressive, precision 8, 160x160, frames 3
Category:	downloaded
Size (bytes):	13897
Entropy (8bit):	7.900268685598436
Encrypted:	false
SSDEEP:	384:hE9ZTKqcnOdNOEX35wsXK/vWqv/CAU7zXwn1sIQcoo43P:hE9oqcOdfX35wsaWqv6HUn1H4P
MD5:	B545C910F9993F7F930513DB793F4EE0
SHA1:	1FF566B853D1C1667852B565D263F3B677F7CF95
SHA-256:	A797D6446620B867248B43792B9AA457B42ADBB7099D9B3129E0D7743DAF67ED
SHA-512:	12A3A9EC217F8B05151D2BDC76B6B2942C86098F1182AD76B7119B959B9937ACFCACC0361188CDF17A629B1D4E76985DFC6AB409939496AF62354AE9FCEB162
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/H_VmuFPRwWZ4UrVl0mPztnf3z5U.jpg
Preview:	......JFIF.....H.H....!.Exif..II*.....J.....R...(.....1.....Z...2.....f...z...H.....H.....GIMP 2.10.8.2019:08:01 11:38:22..... ....JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222.. .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..-#".Uj.....b.T..Gj.#..E..XD..0…ML...H....i.UN}.p}?:].pE8&O....*q.~UOR@l&...m;..jJE....v..8.p...Z..f'

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\HdepnBaFj-yarvouFUIlfV4Q9D8.gz[1].js	
Size (bytes):	3201
Entropy (8bit):	5.369958740257869
Encrypted:	false
SSDEEP:	48:rmo6TIPx85uuYPXznTBB0D6e7htJETfD8QJLxDO7KTUx42Z3rtki:sYuYPXznb0DR7dw8QhIWTQrt7
MD5:	4AADD0F43326BAD8EFD82C85B6D9A20E
SHA1:	4093FC4AB9821B646D64C98051A1CF0679CB2188
SHA-256:	968849A1E6AAED249C78B6CF1AF585AB6C8482A8C5398AB1D2DC3CB92E9EA68F
SHA-512:	616B06A6E3B2385E5487C819FC7F595D473B2F14E8CB76EFB894EDEAB3B26D2C9B679A9B275D924BECC37E156C70B0B56126CCFB62C8B23ABBA9DE07BD93D2A
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/HdepnBaFj-yarvouFUIlfV4Q9D8.gz.js
Preview:	var __spreadArrays=this&&this.__spreadArrays||function(){for(var i=0,n=0,r=arguments.length;n<r;n++)i+=arguments[n].length;for(var u=Array(i),f=0,n=0;n<r;n++)for(var e=arguments[n],t=0,o=e.length;t<o;t++,f++)u[f]=e[t];return u};define("clientinst",["require","exports"],function(n,t){function it(){a=0;u()}function u(){var n,s,t,o;e&&clearTimeout(e);for(n in i)if(i.hasOwnProperty(n)){s=n!=_G.IG?_G.IsUrl.replace(_G.IG,n):_G.IsUrl;for(t in i[n])i[n].hasOwnProperty(t)&&(o=b+s+"&TYPE=Event."+t+"&DATA="+f("")+i[n][t]+f("]"),ut(o)||(g().src=o));delete i[n]}typeof r!="undefined"&&r.setTimeout&&(e=r.setTimeout(u,w))}function rt(){return _G!==undefined&&_G.EF!==undefined&&_G.EF.logsb!==undefined&&_G.EF.logsb===1}function ut(n){return rt()?ft(n,""):!1}function ft(n,t){var i="sendBeacon",r=!1;if(navigator&&navigator[i])try{navigator[i](n,t);r=!0}catch(u){}return r}var y,d,i,g,o,p;t.__esModule=!0;t.Wrap=t.Log2=t.LogInstrumented=t.Log=t.LogCustomEvent=void 0;var r=n("env"),s=n("event.native"),h=n("e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\LL4BV3XU.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	60840
Entropy (8bit):	5.760468685018547
Encrypted:	false
SSDEEP:	1536:GKrSCXrLQPo3H/8cpUQKqETOuKsIecFXdAjvd894fJLYv/pGYdDb097Q53Opw:GGLQw3f/mQKbd89RHpnew
MD5:	C1C8945D755B61FABD7B9809A26DE2B5
SHA1:	E11404380C6E04F07F897AC0E549A5DB50A762B6
SHA-256:	9B8E3EE8C1233000F2C6202FF7A66791E6449762AF606246FBAE19899E14BEE6
SHA-512:	7A2D7328EEF7F754BA22ACAC5EBAD3939EF0485DBD74372973851032245B6E4C33181D56F2426863F03AC47B538334C9C2F851C7AC9064CD4FDDA884290C545
Malicious:	false
Preview:	<!doctype html><html lang="en" dir="ltr"><head><meta name="theme-color" content="#4F4F4F" /><meta name="description" content="Bing helps you turn information in to action, making it faster and easier to go from searching to doing." /><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta name="viewport" content="width=device-width, initial-scale=1.0" /><meta property="fb:app_id" content="570810223073062" /><meta property="og:type" content="website" /><meta property="og:title" content="Info" /><meta property="og:image" content="https://www.bing.com/th?id=OHR.Olympics125_ROW9889344454_tmb.jpg&rf=" /><meta property="og:image:width" content="1366" /><meta property="og:image:height" content="768" /><meta property="og:url" content="https://www.bing.com/?form=HPFBBK&ssd=20210406_0700&mkt=de-CH" /><meta property="og:site_name" content="Bing" /><meta property="og:description" content="The first modern Olympic Games were held 125 years" /><title>Bing</title><link rel="shortcut i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\MDr1f9aJs4rBVf1F5DAtlALvweY.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	257
Entropy (8bit):	4.781091704776374
Encrypted:	false
SSDEEP:	3:qMH4WXMHwmnIB4JmhyfAIB4Jmml0X2IUJIB4JrNOsK1A4JWW7jKYHVA4JRGYdA4S:q6XzD4jr43ldI74FNQlNj7jM9TlMlbSr
MD5:	51A9EA95D5ED461ED98AC3D23A66AA15
SHA1:	62FBB857B873BD79BEE7F16D0766A452FA2798A3
SHA-256:	A5B4181611E951FAECD6C164D704569C633E95FE68D3D1934B911A089EBF70E8
SHA-512:	CEE4231894F82627E50EC746D7C150E5303A1BF8864D7B084173B9D17663A27CC2915F5D0D4DC0602FE26D9EAA10DD98CF3422E7601F520EF34D45C9A506D6F
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/MDr1f9aJs4rBVf1F5DAtlALvweY.gz.js
Preview:	var BM=BM||{};BM.rules={"#sc_hdu":[-1,-1,1],"#hp_id_hdr":[-1,-1,1],"#hp_container":[-1,-1,1],".hp_sw_logo":[-1,-1,0],".b_searchboxForm":[-1,-1,0],"#crs_pane":[-1,-1,0],"#sb_foot":[-1,-1,0],"#sh_rdiv":[-1,-1,0],"img,div[data-src]":[-1,-1,0],iframe:[-1,-1,0]}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\P3LN8DHh0udC9Pbh8UHnw5FJ8R8.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	1516
Entropy (8bit):	5.30762660027466
Encrypted:	false
SSDEEP:	24:+FE64YTsQF61KWlWeM2lSoiLKiUfpIYdk+fzvOMuHMH34tDO8XgGQE3BUf4JPwk:+FdF6UYXEBi9kIHIB1UY
MD5:	EF3DA257078C6DD8C4825032B4375869
SHA1:	35FE0961C2CAF7666A38F2D1DE2B4B5EC75310A1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\P3LN8DHh0udC9Pbh8UHnw5FJ8R8.gz[1].js	
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\9026IKNJ\RrvsBuqGHDpqG7NAz4Q0BMOqQBg.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	4140
Entropy (8bit):	5.268233767834181
Encrypted:	false
SSDEEP:	96:cithlPK4kMRX+1XewlYONYyuGNc22nDmSOsDg:ciJALYONEGNc22nbOsDg
MD5:	7651609B4BE35F5DE8024F570EF6CF87
SHA1:	4B72E4BB1D8F170D6B17FA1D769584A7D0F02F70
SHA-256:	4CA5C607D14D17F8A9EEA9FB0A624BC00C49BFDFBB6A78E1292EAE1461B7D9F0
SHA-512:	7BE114BD02AA079F01FBFC343811F74896BB247ABB79C67998B7DB0F20F8ED1260DEA83523F61CDD0E2231F2428437F9FBF88F39DAD821A3F09A5116C5DA7A2
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/RrvsBuqGHDpqG7NAz4Q0BMOqQBg.gz.js
Preview:	var Feedback;(function(n){var t;(function(){function r(i,r,u,f,e,o){i=typeof i===t?!1:i;i&&scrollTo(0,0);u=typeof u===t?!0:u;n.PackageLoad.Load(r,u,f,e,o)}function e(n,t){for(var r=0,i=null;n&&n.getAttribute&&(!(t>=1)||r<t);){if(i=n.getAttribute("data-fbhlsel"),i!=null)break;r++;n=n.parentNode}return i}var u="feedbackformrequested",c="feedbackInitialized",i,f="",o="feedback-binded",s="clicked",t="undefined",h;n.Bootstrap.InitializeFeedback=function(l,a,v,y,p,w,b,k){function tt(t){var r=null,i;return t&&(i=new h,n.fel("ajax.feedback.collectsettings","gsf",i),r=i.findSettings(t)),r}var d=_ge(a),g,nt;d&&d.classList&&d.classList.contains(o)||(p=typeof p===t?!1:p,g=e(d,3),f!=="sb_feedback"&&(f=a,typeof sj_evt!==t&&(i&&sj_evt.unbind(u,i),i=function(n){var u=null,t=null,f=null,o,i,s;n&&n.length>1&&(i=n[1],i.tagName!==undefined&&i.nodeType!==undefined?(u=i,t=tt(u)):t=i,o=t&&t.elementToHighlight||u,f=e(o));s=t&&t.linkId||a;r(y,l,v,s,f,t)},sj_evt.bind(u,i,1)),typeof SearchAppWrapper!==t&&SearchA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\UYtUYDcn1oZlFG-YfBPz59zejYI[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	964
Entropy (8bit):	4.421237058266115
Encrypted:	false
SSDEEP:	24:t741nTY2jmYXhgauOwgXl3gHuWg9cZLzix9QiVCVCTikxQmQ6Nkpgeoo7:dQnkwXhnuOwIlwHuW7nC9QkaUzQm3Nk5
MD5:	88E3ED3DD7EEE133F73FFB9D36B04B6F
SHA1:	518B54603727D68665146F987C13F3E7DCDE8D82
SHA-256:	A39AB0A67C08D907EDDB18741460399232202C26648D676A22AD06E9C1D874CB
SHA-512:	90FF1284A7FEB9555DFC869644BD5DF8A022AE7873547292D8F6A31BA0808613B6A7F23CB416572ADB298EEE0998E0270B78F41C619D84AB379D0CA9D1D9DA6
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/UYtUYDcn1oZlFG-YfBPz59zejYI.svg
Preview:	<svg focusable="false" xmlns="http://www.w3.org/2000/svg" viewBox="0 0 16 16" enable-background="new 0 0 16 16"><g fill="#00809D"><path d="M2.25 0h-1.25c-.263 0-.521.107-.707.293-.186.186-.293.444-.293.707v1.25c0 .552.448 1 1 1s1-.448 1-1v-.25h.25c.552 0 1-.448 1-1s-.448-1-1-1zM1 8.75c.552 0 1-.448 1-1v-1.5c0-.552-.448-1-1-1s-1 .448-1 1v1.5c0 .552.448 1 1 1zM2.25 12h-.25v-.25c0-.552-.448-1-1-1s-1 .448-1 1v1.25c0 .263.107.521.293.707s.444.293.707.293h1.25c.552 0 1-.448 1-1s-.448-1-1-1zM11.75 2h.25v.25c0 .552.448 1 1 1s1-.448 1-1v-1.25c0-.263-.107-.521-.293-.707-.186-.186-.444-.293-.707-.293h-1.25c-.552 0-1 .448-1 1s.448 1 1 1zM6.25 2h1.5c.552 0 1-.448 1-1s-.448-1-1-1h-1.5c-.552 0-1 .448-1 1s.448 1 1 1zM14.5 7h-.5v-.75c0-.552-.448-1-1-1s-1 .448-1 1v.75h-3.5c-.828 0-1.5.671-1.5 1.5v3.5h-.75c-.552 0-1 .448-1 1s.448 1 1 1h.75v.5c0 .828.672 1.5 1.5 1.5h6c.828 0 1.5-.672 1.5-1.5v-6c0-.829-.672-1.5-1.5-1.5z"/></g><path fill="none" d="M0 0h16v16h-16z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Xp-HPHGHOZznHBwdn7OWdva404Y.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	576
Entropy (8bit):	5.192163014367754
Encrypted:	false
SSDEEP:	12:9mPi891gAseP24yXNbdPd1dPkelrR5MdKIKG/OgrfYc3tOfIvHbt:9mPlP5smDy1dV1dHrLMdKIKG/OgLYgtV
MD5:	F5712E664873FDE8EE9044F693CD2DB7
SHA1:	2A30817F3B99E3BE735F4F85BB66DD5EDF6A89F4
SHA-256:	1562669AD323019CDA49A6CF3BDDECE1672282E7275F9D963031B30EA845FFB2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Xp-HPHGHOZznHBwdn7OWdva404Y.gz[1].js	
SHA-512:	CA0EB961E52D37CAA75F0F22012C045876A8B1A69DB583FE3232EA6A7787A85BEABC282F104C9FD236DA9A500BA15FDF7BD83C1639BFD73EF8EB6A910B75290D
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/Xp-HPHGHOZznHBwdn7OWdva404Y.gz.js
Preview:	var SsoFrame;(function(n){function t(n){if(n&&n.url&&n.sandbox){var t=sj_ce("iframe"),i=t.style;i.visibility="hidden";i.position="absolute";i.height="0";i.width="0";i.border="none";t.src=decodeURIComponent(n.url);t.id="aadssofr";t.setAttribute("sandbox",n.sandbox);_d.body.appendChild(t);n.currentEpoch&&sj_cook.set("SRCHUSR","T",n.currentEpoch,!0,"/");Log&&Log.Log&&Log.Log("ClientInst","NoSignInAttempt","OrgId",!1)}}function i(n){try{n&&n.length===2&&t(n[1])}catch(i){}}n.createFrame=t;n.ssoFrameEntry=i;sj_evt.bind("ssoFrameExists",i,!0,null,!1)})(SsoFrame||(SsoFrame={}))

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\b4Jy0kwhnsWcsDQyuzAEsN7RmhQ[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=5, xresolution=74, yresolution=82, resolutionunit=2, software=GIMP 2.10.8, datetime=2019:07:31 17:59:08], progressive, precision 8, 160x160, frames 3
Category:	downloaded
Size (bytes):	14848
Entropy (8bit):	7.9161237402148545
Encrypted:	false
SSDEEP:	192:d5KKqPy60pSDqRxY0cKZR+dG0cDizbS4z0GoJmsrod96rIE1KRCLHXl4DPzEmISD:dg9PJvoe0LsG0IiF+TVERCjgEmgDG
MD5:	094FAB391B9B906B8A88922CE6827471
SHA1:	6F8272D24C219EC59CB03432BB3004B0DED19A14
SHA-256:	E7DAFF9BBB32681540E010FB10BA87D51938B42B275D0C422E253CED0DD96B79
SHA-512:	B0BE13E1A3E4B5758DFF4B36C1FF49020565FD316295A7413E5312FB90B0EE4B7D93B4FE4AC5DBB4F122E4CAC0705307A29DA52DBF66A3AC0DA91CC94F5B3EF4
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/b4Jy0kwhnsWcsDQyuzAEsN7RmhQ.jpg
Preview:	......JFIF.....H.H....#JExif..II*.....J.....R...(.....1.....Z...2.....f...z...H.....H.....GIMP 2.10.8.2019:07:31 17:59:08.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=9002
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\down[1]	
Preview:	.PNG.....IHDR.....ex....PLTE....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\9026IKNJ\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\9026IKNJ\kBH4DSEA84cgV7IKw7_Bwvm2NpI[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=5, xresolution=74, yresolution=82, resolutionunit=2, software=GIMP 2.10.8, datetime=2019:07:31 17:58:04], progressive, precision 8, 160x160, frames 3
Category:	downloaded
Size (bytes):	11847
Entropy (8bit):	7.82741108986083
Encrypted:	false
SSDEEP:	192:dhK4s5Is9xn1pwLz+SHW36K+Oas6GKNQsjM+N7WzAVrzj+cq615Te+Se:d4ZOOloH/HW3Rp5Ka2tWzAVrzjv55ia
MD5:	5CCC9B225B51915169D6F4C27FA26C9A
SHA1:	9011F80D2100F3872057B20AC3BFC1C2F9B63692
SHA-256:	10D8D2141A01589A82B139B01A75B74D9DFAB16D273C9B2EC7F5087D3EF16B3B
SHA-512:	E2AEB96F6FEC6710AAFF6E52CC24E773CD194F9DEE1BC01FEED88A8EC48033DD9BD8AD0A18C14502DCB6A6ECF05418F18D125E00C4E0E06533495A00F3AF4 11F
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/kBH4DSEA84cgV7IKw7_Bwvm2NpI.jpg
Preview:	......JFIF.....H.H.....Exif..II*.....J.....R...(.....1.....Z...2.....f...z...H.....H.....GIMP 2.10.8.2019:07:31 17:58:04..... .....JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222.. ....."....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...LT...{..3....P.1F)....1N....b.S.F(....;.b...\S.F(.....Q..n(.?.b...1O...cqF)....R.1@....b....R.\P.1K.v(. ..\S

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\model[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	16168
Entropy (8bit):	5.527579595880806
Encrypted:	false
SSDEEP:	384:HUQyIePm3yt9YYQ5bV5u5hOuKsVMhu3kx0m4iDewY/rfrEraIO1uYPW:0yZ3yjYY85uTOuKsV2u3kx0m4iDewY/i
MD5:	B12C190DFA30C8EF3CACFB2304F8A6BB
SHA1:	4485BA9BCEC741F844120DA43AD4C67EED5EFF0F
SHA-256:	E18575EBB4698CD7418A52E923B8815AA1B288FB160F12A9B8DFE69C816FCA67
SHA-512:	0BE8328FD43826911A8BDD74E85C052F47EA08AF97F36C5C8296648B037C60CFEDA186F81A08C1620728FD50F5D3F36C634CCD2D943C41BEE3DDF3F69515B73
Malicious:	false
IE Cache URL:	http://https://www.bing.com/hp/api/model?form=REDIRERR

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\model[1].json	
Preview:	{"ClientSettings":{"Pn":{"Cn":1,"St":0,"Qs":0,"Prod":"P"},"Sc":{"Cn":1,"St":0,"Qs":0,"Prod":"H"},"Qz":{"Cn":1,"St":0,"Qs":0,"Prod":"T"},"Ap":true,"Mute":true,"Lad":"2021-04-06T00:00:00Z","Iotd":0,"Dft":null,"Mvs":0,"Flt":0,"Imp":2},"MediaContents":[{"ImageContent":{"Description":"The first modern Olympic Games were held 125 years ago in Athens in 1896 . 1,500 years after they were banned by the Roman Emperor. The 1896 Games were held in the Panathenaic Stadium, in the shadow of the Acropolis of Athens, shown here. They included athletes from 14 countries, with the largest delegations from Greece, Germany, France and Great Britain. The 43 events included a marathon, tennis, cycling, fencing, shooting, Greco-Roman wrestling and swimming. And while some things haven't changed over the years, some were different back then. Swimmers were taken out to sea by boat for the longer races and had to swim back to shore. Winners were given a silver medal (copper for second place), as well as an o

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\msnpopularnow[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	10423
Entropy (8bit):	5.524868443864616
Encrypted:	false
SSDEEP:	192:uIrvLoZvJZvtcwyltHEZdrXgsqBtCQv6SHGjHHAHaBaZvkr1qPUaDQAbSE5A3GMQ:uOUzaDePrwsUBS/k6Ba52qPJQZEKbNSZ
MD5:	54CD333FA1228D57F2DAEB0617134235
SHA1:	CBA447E953F17FB044B4455A0E36916F1E264E4E
SHA-256:	C0EAE134519D55C8FC8C1E86772F43569FB54FFA44DF785E387F3CC48D106DCD
SHA-512:	4A997C3509A3C5795F39526435886C3F37DB5BE8F11589324075BA689E0770B84F1071288E4EE6AA33E85CFEAF1FA3914E42C4CEE45F740CA1F25AE3AFE7ABD3
Malicious:	false
IE Cache URL:	http://https://www.bing.com/hp/api/v1/msnpopularnow?&format=json&ecount=20&efirst=0&&form=REDIRERR
Preview:	{"title":"","data":[{"typeName":"Msn","items":[{"url":"https://www.msn.com/de-ch/finanzen/top-stories/staatliche-regulierung-allianz-gegen-big-tech-druck-auf-facebook-und-google-w.chst/ar-BB1fkLCT?ocid=BingHPC","imageUrl":"/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkGpp.img&ehk=EoXsvHvTz25OeDlk8%2f1AsQ0JRbPiNyy0iD13c2N9OGI%3d&w=150&h=150&c=8&rs=2&pid=WP0","shortTitle":"Handelsblatt","longTitle":"Staatliche Regulierung: Allianz gegen Big Tech: Druck auf Facebo.","accessibilityTitle":"","subtext":"","isRecommendedNews":false},{"url":"https://www.msn.com/de-ch/news/other/polizei-sucht-mit-superpuma-nach-vermissten-minderj.hrigen-person/ar-BB1flh1z?ocid=BingHPC","imageUrl":"/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1flksC.img&ehk=H0FCoWHkkRHx9dwEmzqiKOqgx9bfKAuVCxCQfuDoLvw%3d&w=150&h=150&c=8&rs=2&pid=WP0","shortTitle":"20 Minuten","longTitle":"Polizei sucht mit Superpuma nach vermissten minderj.hrigen Pe.","acc

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\sbi[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	46137
Entropy (8bit):	5.492718429280291
Encrypted:	false
SSDEEP:	768:WkuL2ym/YIZE2u1U5l7Ez+YIdQFSO4FWCPPZPzATfZjFwummSczZxG3IuO7JUDWB:plB1FWCpPwkNijuSjyir
MD5:	8147A3C6CCDAD2147CA32BA6DB54E40A
SHA1:	3257CCC8CED1107ACBE3697B61F1C5ED3A86A4E6
SHA-256:	E783F26B771F68588FF468DE04C50E6A3E7BC4A11FEBDB52A17511E9DFE91297
SHA-512:	005695CB7F9FBB397109F11FDD375F23D5C678C7F26036E3937C916F75C96857F6A7C1B10D5820588461479A14B69026A3277389E5C02D09359D5A2BD9CF3C67
Malicious:	false
IE Cache URL:	http://https://www.bing.com/images/sbi?mmasync=1&ptn=Homepage&IID=SBI&IG=7461D1DF8734436CBE2E7591A1520DFE&form=REDIRERR
Preview:	<style type="text/css">#sbiarea,#sbicom{display:none}.hassbi #sbiarea{display:inline-block}#sbiarea{margin:0 0 0 18px}.sbox #sb_form #sbiarea{margin:0}#sb_sbi{display:inline-block;cursor:pointer}img#sbi_b{vertical-align:-2px;height:20px;width:20px}#detailPage #detailheader img#sbi_b,.blue2#miniheader img#sbi_b,.sbox img#sbi_b{vertical-align:-3px}.blue2#miniheader img#sbi_b{vertical-align:-1px}#sbi_b.grayscaled{filter:grayscale(1) brightness(1.4);-webkit-filter:grayscale(1) brightness(1.4)}#sbi_b.grayscaled:hover{filter:grayscale(1) brightness(1);-webkit-filter:grayscale(1) brightness(1)}#sb_sbip[shdlg] #sbi_b{filter:grayscale(0);-webkit-filter:grayscale(0)}#sb_sbip .rms_iac{display:inline-block}#sb_sbip:not(.disableTooltip):hover::before,#sb_sbip.shtip:not(.disableTooltip)::before,#sb_sbip[vptest]::before{bottom:-27px;left:10px;z-index:6}#sb_sbip:not(.disableTooltip):hover::after,#sb_sbip.shtip:not(.disableTooltip)::after,#sb_sbip[vptest]::after{top:40px;left:10px;z-index:4}#hp_contain

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\test[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	64
Entropy (8bit):	4.373593025747649
Encrypted:	false
SSDEEP:	3:UMs1TE5LH0cHrJU4YCf:U37cVUof
MD5:	E82D9BD501B46DF5CB2B650AF9E1B126
SHA1:	0FE6876226E88D8104ED51CB6329EB172BBA8D68
SHA-256:	C2BA8FCCFC980BCC8FC24E7A41BFCFEE88CCA9331C8D4D62890D7DFAB4A12226
SHA-512:	D3715E6A3C9012F2D8E1269E5C4B3E2F77FD2CD8E793AD39E51F1E1BE30F0818DDD01FAF3708EF789FDF347B92C6477C10A1155DEC582FF68185CBFD41C662 4
Malicious:	false
Preview:	IPv6Tests.TestIPv6Response('{"type": "4"}');

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\th[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 1920x1080, frames 3
Category:	downloaded
Size (bytes):	344983
Entropy (8bit):	7.987666031914428
Encrypted:	false
SSDEEP:	6144:uhr6bFSzjuZdOJGR0u6FY7Kq1u9ktnbQ9uJ4g2FUXoIQc1tYJsDr0j:AwFEjSOJbuYphkZQ9uJX22TQc1qJwa
MD5:	DDCE5ED235CCBFFDA3F3735F75F80C0F
SHA1:	F266C24FA6F01459F51C97ADB00523BD214C653C
SHA-256:	78EB4A3213EBE7BB95F87D206AE29064D514628E6A430334D0E13756AA131DE5
SHA-512:	A0C70871BC52467524A0107F09B93C1BE11FFBD9CF68E1F3C567F97B0F810AA5B0CEE584AE1BA720F4A0B30F42E4290A06E99B9EA640437B0DABF158F2DB0625
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkU9t.img&ehk=mxhBThhQVDlo%2bCYW2VhueyqJguPlSKZ1mWMM3nr17PY%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....C..... "" .,,,.3333333333...C..... ....## ##,,),.3333333333.....8...."..... S..... ....!1A.."Q2aq..B...#R...b.3r....$C.....4Scs..%DT...u.5t..... B..... !..1AQ."aq.2..... BR..#br.$34..C....Ss...c..... ?.#...9.%qx..fL.Z..+p.....+...X .2m..,..X.<..W...}Dk.\J....f9.~.....b.../.7C&.V.Y.9`.|.rV0'>.9..... 3._>.6.@...ML-...+].Q..... ]..... '>.`e..W>.9..... |.d...>.9..VJ.Es./.%e.....,..y.7.....l..... g.4.3g)..d.99Bk....+r. :e$.ca.SH.|..... m...}.YRO9...j.vd..9V..5..@e...{.<hA...:..... 9K#..... q.H...`....q>NiF=.[..2C.8X...*..... L(.{..... s.3.W.!....{^..'..~....9.!..^A.y...1.A..[..... l!a....i ..)L.D.D.8#.{../.0.\.M. .r..qg3...t.N..^....L.I3'..... eQ.`3{..... Yh...sK...k..I...m.o.t^%e...O..e&a..... 9..v.x....&.E!.e..p..... n.UQ.x$S\..... 1}DqH

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\th[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	2542
Entropy (8bit):	7.7794956985553245
Encrypted:	false
SSDEEP:	48:5yYcuERATBsC87tpyXKeyzbOZkEPVEGYI0Z8RV8WdxGAia:5PECCC87jyXK7ejRWSRV/dxGva
MD5:	357F88390923FD2D7C54F8EF73A57475
SHA1:	EE6F5D3CBE310AC210CF47D8F1B748B2B0B5205E
SHA-256:	80076FB2A8BD57B72985F5F3557F2B4742DE360994CD05CCA6604653E63404E0
SHA-512:	2AE5C52C81E088CEA10B4240BDF45220AEAC3C4BFDEEC6C098F946BA569AE626E753F7CC116FF133C920C14DBC94083B484A3FA045EC226A32F62D69F85D05C
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fl5aC.img&ehk=hx9sEjlDgrlxhlQ0dXS9BWLt7M4%2fn9L%2foLPShsm8wa4%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....H.H.....C..... $ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C..... =)#)=========== .. .."..... }..... !1A..Qa."q.2....#B...R..$3br..... %&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... ..... w..... !1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... ..... ?..(...7..(.....d..0..ci.0.H.8.4ow;F..b[ws.....q...r..@...3L_7..?n.....?LV..d?...J+".....)(..... E8.....W.....F,..JZ..Z)(..... J...fv.....@$...0.cn..q.N{g..:...RCp.. 2aG.lI.T..S..... w .9..V...h.E..aE.....(...(..4.J..K../J(N.WB1{..E..I-....(4Q@...[M.0..... 18....[..Z..... W.J._.#...;s.q...v..... W.I+kr.-%.#.(...(...(...j`<..:.[.a:QH.WJ1{.....c`.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\th[3].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	3742
Entropy (8bit):	7.867632755628144
Encrypted:	false
SSDEEP:	48:pyYcuERAFyZuPbJdd/1D9uU8lPjsEO/pjKnTLdyW+Tm8bV8SANcggbCPdXBUAxaB:pPECyZ6DEU8SEOOLuSMHBggupBBYBzf
MD5:	76A08CC374F645ADFD2D574AEA9E1F67
SHA1:	EF6301792289F45E1914290BD3901BE5C3C08ED7
SHA-256:	6D4A8E2E63961DF63F503AC5A323D9FAD4F738E8720BD98C9A302794CB62847C
SHA-512:	19AADD5296DEA0C5F8D8165911C2ABF00A7BED8E98C7090448664715E99559D92DE6D6196EBE8D7A546A33704BD36A596A85F847DFFBAA3C2BC6E818707F31EA
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fjVGq.img&ehk=CUJArgAlYOIs%2fdufnie%2fHn0v5FuoJklhhKQfEtkFJ8l%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....,.....C..... $ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C..... =)#)=========== .. .."..... }..... !1A..Qa."q.2....#B...R..$3br..... %&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... ..... w..... !1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... ..... ?..r).r)..4..T..(..... '....m.m./....cjd..$D ..v...qj..... }+SN.}.p.Y.F..*[CQfI.Y..1.....>.....!..8..2@.U....Yn.9..F..[....0.o.#)R.@....z3..o..$..3.1....{..%OQ... ...S..!$}.{}k..... y....-Y.KF)qV .!....G....|..K.@.R.J.3.-S(..W..~*.....+CD...lZ..(d...P.b.?6.P3....Q.j7.}.4t..... 8..... X.YC5.ae.....V"....n.0'..i.`.....a.v (fo....S....S\.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\uYzy_SF_Qx-quOm8IecsaqSoOd0[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1400
Entropy (8bit):	4.810462023135915
Encrypted:	false
SSDEEP:	24:t4LxHXU4dxCey0fA53J/S/7/sG5BmefEqrR5GTGOby2NF2E/:+x3U4S55Z/aB5BmefEqrRYK6
MD5:	2C4837A751CDB1A7366A56A0BD33EF59
SHA1:	B98CF2FD217F431FAAB8E9BC21E72C6AA4A839DD
SHA-256:	AA593C656009A40AC1782DD6FEE1EF31F9D4CCAD9F3F657DDF9A72C1EB7E553A
SHA-512:	79DBB36F29034FCB52BA9C51A01346F9CEA694CAEBA9B149EEB66DB732B73C01C71FB7F4FBA892E67523E955153FAE4D0148C1024291CBBA0CBFC26FC5C864 1E
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/uYzy_SF_Qx-quOm8IecsaqSoOd0.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" viewBox="0 0 40 40" style="width:64px;height:64px;">.. <style type="text/css">.. .anim {.. animation-name: blink;.. animation-duration: 1s;.. animation-iteration-count: infinite;.. fill: #05E9F5;.. transition-timing-function: linear;.. }.. @k eyframes blink {.. 0% {.. opacity: 0.. }.. 50% {.. opacity: 1.. }.. 75% {.. opacity: 1.. }.. 100% {.. opacity: 1.. }.. }.. .delay1 {.. animation-delay: 0s;.. }.. .delay2 {.. animation-delay: .125s;.. }.. .delay3 {.. animation-delay: .25s;.. }.. .delay4 {.. animation-delay: .375s;.. }.. .delay5 {.. animation-delay: .5s;.. }.. .delay6 {.. animation-delay: .675s;.. }.. .delay7 {.. animation-delay: .75s;.. }.. .delay8 {.. animation-delay: .875s;.. }.. </style>.. <circle class="delay1 anim" cx="20" cy="8" r="3" />.. <circle class="dela

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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/7H2DIZWYeIsrGYyKYx7
MD5:	4E67D347D439EEB1438AA8C0BF671B6B
SHA1:	E6BA86968328F78BF7BF03554793ACC4335DF1DD
SHA-256:	74DEB89D481050FD76A788660674BEA6C2A06B9272D19BC15F4732571502D94A
SHA-512:	BE40E5C7BB0E9F4C1687FFDDBD1FC16F1D2B19B40AB4865BE81DD5CF5F2D8F469E090219A5814B8DAED3E2CD711D4532E648664BFA601D1FF7BBAA83392D3 0E
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/5rqGloMo94v3vwNVR5OsxDNd8d0.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 32 32"><title>UserSignedOutIcon</title><circle cx="16" cy="16" r="16" fill="#eee"/><path d="M12.73 13.1a3.271 3.271 0 1 1 3.27 3.2 3.237 3.237 0 0 1-3.27-3.2zm-2.73 9.069h1.088a4.91 4.91 0 0 1 9.818 0h1.094a5.884 5.884 0 0 0-3.738-5.434 4.238 4.238 0 0 0 2.1-3.635 4.366 4.366 0 0 0-8.73 0 4.238 4.238 0 0 0 2.1 3.635 5.878 5.878 0 0 0-3.732 5.434z" fill="#666"/><path fill="none" d="M0 0h32v32h-32z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\Jl2vUSlElqWjk-99MuYp4W74zvQ[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1529
Entropy (8bit):	4.135964697042234
Encrypted:	false
SSDEEP:	24:tVvnjuJOeUsc4wg5a2/gt+lm/3HljKR99U1TrD3ptYZ7GDlh6mI0jeI4dIwDq8rz:rn1edcjg5pm/lKRXU1TrD5tJf6mzjidJ
MD5:	6D8EF11CB1C03B39D9ED4E4C9A2190B9
SHA1:	265DAF51294422A5A393EF7D32E629E16EF8CEF4
SHA-256:	D72BEAE30A6B2B36C3E03847CE4EA04211D7373D4066FF937A7A05DF4E0C3DB6
SHA-512:	C8820BDF2FC34CCFF7018A1C1E3E74ED1FE0B287926050F9B6BA59C08DCC216E8732F862AB0BF086BC05275C51E6F81132AFA60F6D50A19585642BC906DCDD 2
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/Jl2vUSlElqWjk-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\CS6IXJW6\KC_nX2_tPPyFvVw1RK20Yu1FyDk[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\KC_nX2_tPPyFvVw1RK20Yu1FyDk[1].svg	
Size (bytes):	726
Entropy (8bit):	4.636787858533541
Encrypted:	false
SSDEEP:	12:tbH41nlcWYiB1+Xl0ML2t1iOfEmmgaUEUZQ6nMAIPWSxs4yPISEIe9t8aayPISEx:t741nTYifqLL2+O7mgaxSQ6MFnE3nkO
MD5:	6601E4A25AB847203E1015B32514B16C
SHA1:	282FE75F6FED3CFC85BD5C3544ADB462ED45C839
SHA-256:	6E5D3FFF70EEC85FF6D42C84062076688CB092A3D605F47260DBBE6B3B836B21
SHA-512:	305C325EAD714D7BCBD25F3ACED4D7B6AED6AE58D7D4C2F2DFFCE3DFDEB0F427EC812639AD50708EA08BC79E4FAD8AC2D9562B142E0808936053715938638 7C
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/KC_nX2_tPPyFvVw1RK20Yu1FyDk.svg
Preview:	<svg focusable="false" xmlns="http://www.w3.org/2000/svg" viewBox="0 0 16 16" enable-background="new 0 0 16 16">.. <path d="M0 0h16v16h-16v-16z" fill="none"/>.. <path fill="#007DAA" d="M11 4h4l-5 4v3c0 .552.447 1 1 1zm-3-1v-3h-4.5c-.828 0-1.5.672-1.5 1.5v13c0 .828.672 1.5 1.5 1.5h10c.828 0 1.5-.672 1.5-1.5v-8.5h-4c-1.654 0-3-1.346-3-3zm4.707 10.707c-.181.181-.431.293-.707.293h-7c-.276 0-.526-.112-.707-.293s-.293-.431-.293-.707.112-.526.293-.707.431-.293.707-.293h7c.276 0 .526.112.707.293s.293.431.293.707-.112.526-.293.707zm0-5.414c.181.181.293.431.293.707s-.112.526-.293.707-.431.293-.707.293h-7c-.276 0-.526-.112-.707-.293s-.293-.431-.293-.707.112-.526.293-.707.431-.293.707-.293h7c.276 0 .526.112.707.293z"/>..</svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\Lq2ZTcK-ZOpjsEJIXReQZG4mDLg.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	67125
Entropy (8bit):	5.23613773666319
Encrypted:	false
SSDEEP:	768:PfY2/W3m6CHbtHgtBkrel21k4Q8BLBSaJBe7BHyJxBCGnVW4nMO51sEBvkH7BSVq:Y2rA3cnq5QPW4nMETv8jYXmNw6V+oF
MD5:	7A6E7F57E8AA30D249A26C481B6CE82C
SHA1:	9902B866538741587475CE0037E4C656F1153D2C
SHA-256:	BAAFA901C91AFC368F4C5443428A247ABE016AD95843AD74148D4321CC0D34DC
SHA-512:	553F287EAEA2583475A96D4F66685C0505FA3961348413F42996631E0F80FC3FF57389EFA6FD5E862F06CAE7110B818BFEED071DF96495CA9EBFB7BCA6FD6162
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/Lq2ZTcK-ZOpjsEJIXReQZG4mDLg.gz.js
Preview:	var AutoSuggest,__extends,Bing,sa_inst;(function(n){var t;(function(n){var t,i,r,u,f,e;(function(n){n.User="SRCHHPGUSR"})(t=n.CookieNames||(n.CookieNames={})),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\CS6IXJW6\MstqcgNaYngCBavkktAoSE0--po.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	391
Entropy (8bit):	5.184440623275194
Encrypted:	false
SSDEEP:	12:2Qxjl/mLAHPWEaaGRHkj6iLUEkFKgs5qHT:2QC8H+aGRHk+i1kFKgs5qHT
MD5:	55EC2297C0CF262C5FA9332F97C1B77A
SHA1:	92640E3D0A7CBE5D47BC8F0F7CC9362E82489D23
SHA-256:	342C3DD52A8A456F53093671D8D91F7AF5B3299D72D60EDB28E4F506368C6467
SHA-512:	D070B9C415298A0F25234D1D7EAFB8BAE0D709590D3C806FCEAEC6631FDA37DFFCA40F785C86C4655AA075522E804B79A7843C647F1E98D97CCE599336DD9D 9
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/MstqcgNaYngCBavkktAoSE0--po.gz.js
Preview:	(function(){function n(){var n=_ge("id_p"),t,i;n&&(t="",i="",n.dataset?(t=n.dataset.src,i=n.dataset.alt):(t=n.getAttribute("data-src"),i=n.getAttribute("data-alt")),t&&t!=""&&(n.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\CS6IXJW6\N55Tc-oLNOuzZam9OghLsR0GD5U[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=6, xresolution=86, yresolution=94, resolutionunit=2, software=GIMP 2.10.18, datetime=2020:04:16 19:04:38], progressive, precision 8, 160x160, frames 3
Category:	downloaded
Size (bytes):	8245
Entropy (8bit):	7.528284902127932
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\N55Tc-oLNOuzZam9OghLsR0GD5U[1].jpg	
SSDEEP:	192:BKWN2AtZTviNV8+xq4UZg11u5FR5CUtlkZPRKY:Yi2aZTvNSU+ODR5CCkRr
MD5:	8BC40A6F56CB4477BFB120A472920EC1
SHA1:	379E5373EA0B34EBB365A9BD3A084BB11D060F95
SHA-256:	9050D49D0786F054BC4B7DA42690B034C208A4736B7DE430383A3333A51C9835
SHA-512:	50CD42440CF3C68FC807338C4F5E3AF681FEE41C0767EE7392F9C21A75D2B6483587E89E048128470DBA92EB054E82459BC16A3B0EE61DD89BAEA11E934EAAE9
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/N55Tc-oLNOuzZam9OghLsR0GD5U.jpg
Preview:	......JFIF.....H.H.....Exif..II*.....V.....^...(.....1.....f...2.....t...i.....H.....H.....GIMP 2.10.18..2020:04:16 19:04:38..... .....JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222 2222222222222222222.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz. .....?...(....(...(....(...(..`.QE..QE..QE..QIH..(...(.....P.E.P.E...QE...QE.-.Q@..R..E.P.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
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\CS6IXJW6\Passport[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	329
Entropy (8bit):	5.086971439676268
Encrypted:	false
SSDEEP:	6:qzxUe3X965+zAqEFtTNfYEAn4TXQ3SOFCL0H4WZhCroOI:kxFkXq6tTRYEVTAx4IHH7CroOI
MD5:	7B7D5DA1B057EB0D5A58C2585E80BACA
SHA1:	29714CD8C570E321C1C1C991E77ACE3945312AC6
SHA-256:	023CD9B7315636BE1BE24DC78144554B0E76777BD476ED581378172DE9B12A05
SHA-512:	1A4E36E3124968166579C04D05A1325242E1DFE20DF4C804081487A019B88395A679A439525488F78B73334C5B0BD38D61E24F8E23F2F8274C6BAC323291CEE8
Malicious:	false
IE Cache URL:	http://https://www.bing.com/secure/Passport.aspx?popup=1&ssl=1
Preview:	<html><head><title>Bing</title></head><body>Loading...<script type="application/x-javascript">//<![CDATA[.var _w = window; var o = _w.opener; var mainWindow; (mainWindow = o) || (mainWindow = _w.parent); if (mainWindow) {mainWindow.sj_evt && mainWindow.sj_evt.fire("wl:cancel"); };if (o) _w.close();;.//]]></script></body></html>

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\ULJCe4CXM2DCjZgELMGm2K4PcPo[1].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\CS6IXJW6\XvRHqJwJt19aXQca73hQTfvNMxk[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	545
Entropy (8bit):	5.028824557535963
Encrypted:	false
SSDEEP:	12:t4102hriVtBr4pFm9z0kjhlHJW1QOYIX+Xw5RxnnS8K0ML2wtp:t41jiVt5wIz0kjhlHJW1QNCRxS8KLL2a
MD5:	58725E06FABDC207D4350D6F3C5B33D0
SHA1:	5EF447A89C09B75F5A5D071AEF78504DFBCD3319
SHA-256:	EDD5715C42AD596AFE1CF07A400D4F33A2F5388C18ADFDD169A7E9467BC9E9DB
SHA-512:	69F8A2161EDE8AA0BE70ECF641D1C05D7E9B5E6952DD41255E02B7AE9FAFDC94A9547DDDB46A2FF9A56C852239558E3C6634D93A1D6D7669C719956C8D2F5D D6
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/XvRHqJwJt19aXQca73hQTfvNMxk.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 20 20" enable-background="new 0 0 20 20">.. <circle fill="#00809D" cx="10" cy="10" r="3"/>.. <circle fill ="#00809D" cx="5.5" cy="5.5" r="1.25"/>.. <path stroke="#00809D" stroke-width="2" stroke-linecap="round" stroke-miterlimit="10" d="M1 7.25v-2.5c0-2.071 1.679-3.75 3.75-3.75h2.5M7.25 19h-2.5c-2.071 0-3.75-1.679-3.75-3.75v-2.5M19 12.75v2.5c0 2.071-1.679 3.75-3.75 3.75h-2.5M12.75 1h2.5c2.071 0 3.75 1.679 3.75 3.75v2.5" f ill="none"/>.. <path fill="none" d="M0 0h20v20h-20z"/>..</svg>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\bLULVERLX4vU6bjspboNMw9vl_0.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	very short file (no magic)
Category:	downloaded
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/bLULVERLX4vU6bjspboNMw9vl_0.gz.js
Preview:	0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	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.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\errorPageStrings[1]	
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 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\CS6IXJW6\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_contai ner"),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){ManagedC ookiePreferenceActio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\k5oM71-Oyo7w7ptkcB_2S5dIr7I.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	21824
Entropy (8bit):	5.243380331742482
Encrypted:	false
SSDEEP:	384:HXpeDC+2uguwBYFsOZrSzz3wp0OxAmzjEHU:HXpeDz2gFsOZrOXWz4HU
MD5:	071CABC528DA3CDD5BD5C7F0EC48ED96
SHA1:	8B665A2DA630D6711E01E838877510F48C40E9CE
SHA-256:	9871F6289648EEA5CB484C2307C4E7BCDF3857AEB27EB07E0ACFD4C1B77EDBB5
SHA-512:	771DA4D3B22B53C5B1B1D2DF1B923B78124A7F92576700F7E988A1E40C2806CB2366D52C556F1FD49862B1A584D871ED7207B54174172740B4ED125AAD4C531F
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/k5oM71-Oyo7w7ptkcB_2S5dIr7I.gz.js
Preview:	(function () {.. if (typeof window !== 'undefined') {.. (function (arr) { arr.forEach(function (item) { if (item.hasOwnProperty('remove')) { return; } Object.defineProper ty(item, 'remove', { configurable: true, enumerable: true, writable: true, value: function remove() { if (this.parentNode === null) { return; } this.parentNode.removeChild(this); } }); }); })([Element.prototype, CharacterData.prototype, DocumentType.prototype]);.... !function(e,n){"object"==typeof exports&&"undefined"!=typeof module?n():"fun ction"==typeof define&&define.amd?define(n):n()}(0,function(){"use strict";function e(e){var n=this.constructor;return this.then(function(t){return n.resolve(e()).then(function() {return t})},function(t){return n.resolve(e()).then(function(){return n.reject(t)})})}function n(e){return!(!e||"undefined"==typeof e.length)}function t(){}function o(e){if(!(this in stanceof o))throw new TypeError("Promises must be constructed via new");if("function"!=typeof e)throw new Type

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\IK_FmcR4naKX9hplwfe9ify1hf4.gz[1].js	
Encrypted:	false
SSDEEP:	1536:ppkCMu1Rv0SuDHT4kfr5IRnO8E9FqJCnq1EoAXycCroA0wT8aHs3:3Mu1Rv0SvNmeGq1ENXdTAVM
MD5:	C24FE194A488B12CCE5B3858D12C2C3D
SHA1:	E55B3E549CA42D614BEE0C4538F9EDA6C89DE00D
SHA-256:	45A1BD96D9A1BB1F03191C2F062FDC5369542864C4777A67623811BE6463D4D6
SHA-512:	4F1C02C2FE716DBEAF061DC9476AD35E33F5C808FD3D79D0ADBECED81B65A02225F7356DBCB10A7232BDD7D02BC0C908F17BB61B058FF5FB99747202522B54 3
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/IK_FmcR4naKX9hplwfe9ify1hf4.gz.js
Preview:	var __assign=this&&this.__assign||function(){return __assign=Object.assign||function(n){for(var t,r,i=1,u=arguments.length;i<u;i++){t=arguments[i];for(r in t)Object.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\CS6IXJW6\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:	E70F996B09E9FA94BA32F83B7AA348DC3A912146F21F9F7A7B5DEEA0F68CF81723AB4FEDF1BA12B46AA4591758339F752A4EBA11539BEB16E0E34AD7EC94676 3
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\CS6IXJW6\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:	E85360DBBB0881792B86DCAF56789434152ED69E00A99202B880F19D551B8C78EEFF38A5836024F5D61DBC36818A39A921957F13FBF592BAAFD06ACB1AED244I
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/pXscrbCrewUD-UetJTvW5F7YMxo.gz.js
Preview:	var BingAtWork;(function(n){var t;(function(n){function t(t,i){var u,r;t.isAuthenticated&&(n.raiseAuthEventAndLog(t),u=_ge("sb_form_q"),u&&(r=u.getAttribute("value"),r&&(n.fetchLowerHeader(r),n.fetchScopeBar(r),i.notifEnabled&&i.notifFetchAsync&&n.fetchNotificationConditional())))}function i(n,i){n&&n.length==2&&t(n[1],i)}n.bindToConditionalSignIn=function(n){sj_evt.bind("ssofirstquery",function(t){return i(t,n)},!0,null,!1)}})(t=n.ConditionalSignIn||(n.ConditionalSignIn={}))})(BingAtWork||(BingAtWork={}))

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\th[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	4103
Entropy (8bit):	7.905624591549082
Encrypted:	false
SSDEEP:	96:pPE7azjJGnUjIWZ3fWfX6c11tzgyuBDgYNgdZ/z:pPQkJHsccXV11tzgDBDgYaz
MD5:	D79048C62D1919EBD68359F962DE7D0C
SHA1:	56CA765E294DD844FCD7D56339AC81647DEF4D8E
SHA-256:	92B97018B5A41B256E26BDCB5764E3076A44FF3B2DD3C89FC3E1C20A024EA559
SHA-512:	1F91EC0DF06E58899F1EC644F654C1CE069DDFC6DFB6B8F545B6C66D71867797D420D899D7152EE99729B86888589E3FBED27CE56277B3B2DB3C4FFD829AEA B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\th[1].jpg	
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fiIcx.img&ehk=u4rkWZofWQoQJ11NQ%2fu8JYLsufAv%2fujiPAfuy3supnc%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....``.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=========..."}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..H..C...7CVWED..1a..-.....<R].O....(..6...w..T.R..mS..6.%.@b.....Uf...C.%.o..T....M..N...]Iw4P..<[.I.3).)$... d{sM..g.V..S...~..W...khU}H..B.)\.!..&'M.F..f.:.'#.tFI..b2)P..U.`..m;.%".....AKE..))i. .....bo.j.....A..4.,...<.K4.$..pOz.....-:..... .'".....v..T.\g.O.=MQ.E..fV..|.l/....U.....ZRB..Q.~..V.....K.o(r.E.....t$.....P.<H..3.~.....{.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\th[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	4602
Entropy (8bit):	7.919085409507157
Encrypted:	false
SSDEEP:	96:pPEQIac5U07wxonYM7ZCOPHZ3V4DItC+Es/YzbvLSLIBpxrDn5M:pPjeyynnlCoZ32In4TL6CHD+
MD5:	8816AF91855EFB0BB97FAF7429A17E5A
SHA1:	7FFA5A24554D8CA448E6D1F98A7AC31F36CB2FC7
SHA-256:	1C54DB3F6FA0501AB0C6ACC1BFFC8629009F76BE5AA6DE4239FEB24E3C6AEBFC
SHA-512:	F615D37B9E117B9E1A8DC287DC4FD5888BE85F8CB9E9C66E49B547A0D3969611771660322511 7D05D7E30734131D15A5C651EFD0B6E9DA546825352B25CCF082
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fjIfk.img&ehk=fogkfx9NpBv%2brwC9WfPL2X5KtkEuDG5AjpDW%2f%2bCifdo%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....``.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=========..."}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..XqBS.N)..i.,'..H..uH..(..(..5H..$..$...u$...j^/..]4.[...h.).z.V...+.jt1.7E'.).V/.....O...(..c.....8...!ei.|.Y.py...4...=...y_Q.....R{G2Z\4,9'".....7.iz.>..p..zP..lz.)....<J.z..P..OZn).H.....h.4P..>(.. S$..J.&.P...(.....e...Py.....mjH...}.#.u..g..@.'.j...v.r.zd..kR..[...$.p.....P.....".b|...9.....8_A.....9.i[J.Y.(#..[.:Ai.<".....k...;d.j:w.\.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\th[3].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	2974
Entropy (8bit):	7.842117922223016
Encrypted:	false
SSDEEP:	48:pyYcuERAaijwRfGEmShUNpHgPW3t9K4kgV90rFGyeKLt8vzC:pPEMMME4NpAe3tUsyhGHKLtR
MD5:	4BA560E225A43E2EF51F8649A0E8C8DE
SHA1:	3FE52097D629F58AD03B273E2CCDC94E6C6BEB2A
SHA-256:	D2598D2530ACA0331C98A18F8F318F70A3109F5D1649181EC7932BA5012CCD57
SHA-512:	0F8B21DCF44D73C7EB3FB81C2E54829C70166594D042DBF989A55A4EA81F5C969F5C8702FA7520C19E94CFD6489486A0E35E68FD5A12EED6BF88C95A55EF159
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fiT16.img&ehk=6BnfE8%2fNfTa0RI%2f5H%2f7p0tBSDWku%2bqsPBIIe2%2bS4aVE%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....``.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=========..."}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..<5Y.<I..j.i.z..?14)..\..D...*.'.....T.)M..i.A..F*y.53'&.....MG.l.K..$i...K,.EQ.Sb .....\.lO%.#...#.?J.S.V.z.....5....)y~...!Ry;..'.q..O.m...g(5.MS..e.*lo.f.B.....nX..2)q.0.....A.<.Tn..eY.4R...^l.....d...D..F+.....8..".d...m..U..O/51^iB.M.:_*..O.E.._*.0>..l..!l.=.._..Q.z....O0..<.VR.....*.GN.uc.nq.U.VV..[.O..+7NQ.8...m.Y..j.m..{.R&3D$...%

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\th[4].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	4702
Entropy (8bit):	7.908846168376892
Encrypted:	false
SSDEEP:	96:5PEIFvu30PKAwj7yYJytXvjuaRu1foTpeYJGC8RYW5Ene:5PrRCAGy5t/juYmfoF7Re1
MD5:	D24AE5FCFFF6F8E79776AC8C41E6B6BA
SHA1:	1162C24A9B13E16B032B61C30924A2FC9CFE1BB0
SHA-256:	397DC263B80321B619D6B2A8240E092B05CEA0988D2D52CA5B229972BC675440
SHA-512:	92257013E49148EE6FB43CF4056AC0A40C72C2B80FC35D44893EF99E36F4D36CEF4790231C38FAD5D99B77A6D5B584400972C8E840A786B6E6B2DE391ECEE75
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\th[4].jpg	
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkq4a.img&ehk=fdwT4sR5PmkMJ8vZsLGghGPVAqp4uF2%2byvEsZ27GA1M%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....H.H.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)==========......"..}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....R....C.E.....Q...,#..xT..9~.}3.P.f..~.....cS.+..!.-....).*.o.:..?;.3..U4<.....>..?..;....G.Zz.IJ..y...9....G).TS6(`..o....j...)oJ.....j)...M?....r..z.C.....%l.*....)...)....QX./..%.'....h.....>QISO..g.NB1P}pj..^..wI.....J~.Z..g.\]xr.A.a_.S@.IZ.....|2.....~.G.y..3^.]...*...:}."..\..x..@.....,..[]..X.....N...k....1}...S...G;.....z.KL.J.....27.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\th[5].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	5718
Entropy (8bit):	7.9318718460651025
Encrypted:	false
SSDEEP:	96:pPEJOqsYH47+dCCG6wRGFkXNcO8XOnW81LsImKDFLMwLXZUIEAWgKhE1:pPeOKH470Cv6wRGFSGO8kZ1L8+oiZUrg
MD5:	5ABBBE53C535080AE3BE91FE6F0B93C1
SHA1:	6A991409D0A6886057BBD0DC9AE71AAFB111E8C1
SHA-256:	B692C27DDDA4FFE62BB2C57AA229EB9298EBDA7726BC227089CEEFDF5E05AD4C
SHA-512:	2283634663D24B2C87399A5C562C5E73C68905BF799FD41367D15E4BCF336B5BA5511706998D9C439016799E56B20E5693BCCECA1D9037223D07659410570EC6
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkfuX.img&ehk=Al75D9k%2bIhZGZEnhR9bRctnjlt4TfOCoHOzqmGEyQNE%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....`.`.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)==========......"..}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..5..Z...9.{...<....[w..G..W7;.....P.-%V.c..L.>....`A..5.i.".i..A.<.k.....^.Z..u.....8.....&.9.I.....&..\l.>Ty(.xs...b.....U.*id...r....}zV...Xk>cm.*.[..5.(.u.F.....P....;.x....{c..mxfR.....fk....;>..]....[H.u.eO.....4<..C..m.a.....J`..c...z....-.`.B._S._....!.....l9.N1...PZ.....z.N...)...M~/.i.p.y.H.b.xP}Y....k.....4.X]).l.Fb

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\th[6].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	6795
Entropy (8bit):	7.939267233088054
Encrypted:	false
SSDEEP:	192:pPFWzMAm+TL7LZ895qWynOjJN52aPjP2D9a1R0:5FWmM7y7TZFNoaLc9Ai
MD5:	140F382635756FE19E1CD67D8CDAB923
SHA1:	1B0F1B61C068E01CE6FFDC5FFCADDD5E039D0DA5
SHA-256:	216E799943B615F3EBF0FC09391810AF53FDE0EDCBEC4300F2B01B98AF346FAE
SHA-512:	A7403C2FB1E2C858C3B3A1F6860441A8B820033E5D6E0049DF6922A1BFB0F74180A2538CFD82F292219629FB1FCA6AB8D3AAAA97129C4C86BC8D15FACDD405f3
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fk3tJ.img&ehk=VNetxfVLBzRQk0Hk9PeD6wuxhnc6QG%2bQVORzTT762Ms%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....,.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)==========......"..}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....3Fj.E.[.$\..M..+.ij.!...{..,.....j\..|.\....>..7.....}kVo.(bD..U...Pj....XO.....$.[..|....<...p._0..n*...k..O...D6.L.`....?..U-..D...f.....h.'z^(...&j...[h:S..."....O.k.o...7..@..`.n.~R.....Px...m ;.3X...E.....D..Cm.$..8>....F(...VrB.1..4S.....u.&.w.Oe3...1.C..2.....1..5.j.....!&._..n.h...'.r.=I..y...Y..2.\....a$...$.;.$..v.,.....YR..%.....;.N

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\4L4QdyjTv0HYE2Ig2ol9eYoqxg8[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1101
Entropy (8bit):	4.829151166001716
Encrypted:	false
SSDEEP:	24:t0S8eLfl954T0u2y3EO1gRcDrIvQaDxijjfscC:vLfRWtPDuQKIjq
MD5:	91CD11CFCCA65CFACE96153268D71F63
SHA1:	E0BE107728D3BF41D8136220DA897D798A2AC60F
SHA-256:	8EE1E6D7A487C38412D7B375AC4A6BD7E47F70858055EEB7957226ADA05544BE
SHA-512:	4367CE147C7FA4590838F23C47819B8954858128336979E28BA116924B92660A7CBDC9A8292C45C5F26FF591F423F03DFADCB78A772DBE86AC5FBABF0B4E7711
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/4L4QdyjTv0HYE2Ig2ol9eYoqxg8.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\4L4QdyjTv0HYE2Ig2oI9eYoqxg8[1].svg	
Preview:	<svg focusable="false" width="24px" height="24px" viewBox="0 0 24 24" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">.. <rect fill-opacity="0.2" fill="#000" x="0" y="0" width="24" height="24" rx="2"></rect>.. <g transform="translate(4, 4)">.. <path d="M13.2916881,1.29304814 L7.99 395739,6.59077883 L2.69622669,1.29304814 C2.30349711,0.913737214 1.67923378,0.919161894 1.29315522,1.30524045 C0.907076669,1.691319 0.901651 99,2.31558234 1.28096291,2.70831192 L6.57869361,8.00604261 L1.28096291,13.3037733 C0.90165199,13.6965029 0.907076669,14.3207662 1.29315522,1 4.7068448 C1.67923378,15.0929233 2.30349711,15.098348 2.69622669,14.7190371 L7.99395739,9.42130639 L13.2916881,14.7190371 C13.6844177,15.098348 14.308681,15.0929233 14.6947596,14.7068448 C15.0808381,14.3207662 15.0862628,13.6965029 14.7069519,13.3037733 L9.40922117,8.00604261 L14.7069519,2 .70831192 C15.0976827,2.31746305 15.0976827,1.683897 14.7069519,1.29304814 C14.316103,0.902317288 13

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\CMm2G4GK3T9XHTMByeN2QI1OVUs[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=5, xresolution=74, yresolution=82, resolutionunit=2, software=GIMP 2.10.8, datetime=2019:07:31 17:51:08], progressive, precisi on 8, 160x158, frames 3
Category:	downloaded
Size (bytes):	12415
Entropy (8bit):	7.878337322573188
Encrypted:	false
SSDEEP:	384:dnoYiTiJAAcGIs8E76ZFIN92VPGeBe+ELS:dnyiCAcGIu2FIN92REm
MD5:	A0BFF1A68EAB91DAC459F3B2EB4B3DE3
SHA1:	08C9B61B818ADD3F571D3301C9E376408D4E554B
SHA-256:	7DB453C22084AEF847E1CA04E9FC1B1CF0D468A5C11ABF3C09968C840CD96A87
SHA-512:	3685F5DD0B8869A0B71C4CADF4FE8559094DC431FEE1E14C349BF6E933702B90136EE45277A97627F69BBB6FAB5ED9EF98AFEBCF88079C5EFFEBD4100B64CE 21
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/CMm2G4GK3T9XHTMByeN2QI1OVUs.jpg
Preview:	......JFIF.....H.H.....>Exif..II*.....J.....R...(.....1.....Z...2.....f...z...H.....H.....GIMP 2.10.8.2019:07:31 17:51:08..... .....P.....JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222 22222222....."....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....,f.iJ..b..vR..6.@...*T..8..0%H...8...cH.I.S.F(.....yZLS.....P..1.,i1F(.s.&.....+..iqR/.(.E.".Q.M)VYiR

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\DCD2HH6I.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):	60840
Entropy (8bit):	5.759943777398637
Encrypted:	false
SSDEEP:	1536:GKrSCXrLQPo3H/8cpUQDqETOuKsIecFXdAjvdC94fJLYvipGYdKb097Q53Opw:GGLQw3f/mQDbdC9RqpWew
MD5:	3749BC27EC70DEB38E54B238BF2B2798
SHA1:	DAC7B3D32D9E51FF35C89E168C09AD3EEBB9F694
SHA-256:	0E77757EE09287A8799367A38E13F7DFEEF02E1ABC2FCA4FBE659718A17C4F3E
SHA-512:	B638435FA45A4AB1B4E99CBAA2B7E2127F4A1D9C28C799C1A8ADFC033ADFF218AAEC295A801246FB141C6627D05B995933671243AF80285AE568E7850CB4A96
Malicious:	false
IE Cache URL:	http://https://www.bing.com/?form=REDIRERR
Preview:	<!doctype html><html lang="en" dir="ltr"><head><meta name="theme-color" content="#4F4F4F" /><meta name="description" content="Bing helps you turn information in to action, making it faster and easier to go from searching to doing." /><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta name="viewport" content="w idth=device-width, initial-scale=1.0" /><meta property="fb:app_id" content="570810223073062" /><meta property="og:type" content="website" /><meta property="og:title" content="Info" /><meta property="og:image" content="https://www.bing.com/th?id=OHR.Olympics125_ROW9889344454_tmb.jpg&rf=" /><meta property="og:image:w idth" content="1366" /><meta property="og:image:height" content="768" /><meta property="og:url" content="https://www.bing.com/?form=HPFBBK&ssd=202 10406_0700&mkt=de-CH" /><meta property="og:site_name" content="Bing" /><meta property="og:description" content="The first modern Olympic Games were held 125 years" /><title>Bing</title><link rel="shortcut i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\Fsa_OI0AplCnVoXGca8ALOo0S0s[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	282
Entropy (8bit):	4.768675821769942
Encrypted:	false
SSDEEP:	6:tbXH4mc4sl3UY7eERI1+N9H5R0MLERlwoVNdJMvdIXyCWfuBIAFfu:tbH41niB1+bj0MLBnpavdqyVGBIAFm
MD5:	E38795B634154EC1FF41C6BCDA54EE52
SHA1:	16C6BF388D00A650A75685C671AF002CEA344B4B
SHA-256:	66B589F920473F0FD69C45C8E3C93A95BB456B219CBA3D52873F2A3A1880F3F0
SHA-512:	DCA2E67C46CFF1B9BE39CE8B0D83C34173E6B77EC08FA4EB4BA18A4555144523C570D785549FED7A9909C2E2C3B48D705B6E332832CA4D5DE424B5F7C3CD5 BE
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/Fsa_OI0AplCnVoXGca8ALOo0S0s.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\Fsa_OI0AplCnVoXGca8ALOo0S0s[1].svg	
Preview:	<svg focusable="false" xmlns="http://www.w3.org/2000/svg" viewBox="0 0 16 16">.. <path d="M0 0h16v16h-16z" fill="none"/>.. <path d="M8 1a7 7 0 1 0 7 7 7 7 0 0 0-7-7zm1 10a1 1 0 0 1-2 0v-3a1 1 0 0 1 2 0zm-.293-5.293a1 1 0 1 1 .293-.707 1 1 0 0 1-.293.707z" fill="#767676"/>..</svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\GiGr-rA9TBhE2c3LJn7PvDweiOo.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	374771
Entropy (8bit):	5.158592433297743
Encrypted:	false
SSDEEP:	6144:1irrzbB3LH7gaV6Z8LAfP0Rp6Izc04YFdNwRm2EjXi4SG7oIBYQmzeH:aHNfi4KwYQmzeH
MD5:	F279A46B56038C41BB3FC11D67D0FE46
SHA1:	B48121E695FD6483CAA7F48DE73FE9F121777109
SHA-256:	A9EA274B393E34591387AC0B4DE594BEE296386543DE34F4897281324DB0DCBB
SHA-512:	4C1754CF5E368D8CE86B135B789A4FF4BAAD1419F30A1EB3B65EAB62217C054D0066EA5FC22B5AA7643EA959854EBC2029B39CB7D1AEAAFB78B95A2A46430F84
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/GiGr-rA9TBhE2c3LJn7PvDweiOo.gz.js
Preview:	(function(n){function t(r){if(i[r])return i[r].exports;var u=i[r]={i:r,l:!1,exports:{}};return n[r].call(u.exports,u,u.exports,t),u.l=!0,u.exports}var i={};return t.m=n,t.c=i,t.d=function(n,i,r){t.o(n,i)||Object.defineProperty(n,i,{enumerable:!0,get:r})},t.r=function(n){typeof Symbol!="undefined"&&Symbol.toStringTag&&Object.defineProperty(n,Symbol.toStringTag,{value:"Module"});Object.defineProperty(n,"__esModule",{value:!0})},t.t=function(n,i){var r,u;if((i&1&&(n=t(n)),i&8)||i&4&&typeof n=="object"&&n&&n.__esModule)return n;if(r=Object.create(null),t.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:n}),i&2&&typeof n!="string")for(u in n)t.d(r,u,function(t){return n[t]}.bind(null,u));return r},t.n=function(n){var i=n&&n.__esModule?function(){return n["default"]}:function(){return n};return t.d(i,"a",i),i},t.o=function(n,t){return Object.prototype.hasOwnProperty.call(n,t)},t.p="",t(t.s=0)})([function(n,t,i){window.SpeechSDK=i(1)},function(n,t,i){"use strict";function r(n){for(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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
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\OR0WKIO1\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\OR0WKIO1\cs[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):	366
Entropy (8bit):	7.298537550431743
Encrypted:	false
SSDEEP:	6:XtW79fWRvABRSN+NvJTetFwXK+7lKsBlr0KsCF8inFgwqba3IFaenlhH/:XkdWRFN+NhTeMa+BVBlIoFnFFx3SlR/
MD5:	66C999098FC5696E13F910C689766CCB
SHA1:	3F6BC7BDD95E0A4AD706D7F59BBDA28D622FCAC1
SHA-256:	94C848E65844A437363C0E79BD1E7CBEA0886139AD7D27788E1FC98B48C88362
SHA-512:	15B038DC316670123D9E42DA99FA72F77F8328DF9A052AE9EC0BC9C314740EDA0DC5702C689DD6E4AA861AD33FB445EB68A86D979A82935CAC6D72E9D603375
Malicious:	false
Preview:	.....T..S.@.@...?8.:.....HL.R.....@+..}S...y...W.....CT.....UO.m..1..F&7_.....S.G..oX1..JU.7.].....R....;).!..-z.]+....J...]...rq.....}..^..D..;_N`.V.Gm..#7.....cun..d...v.W.i .....:Q.I^.s.9[#...BzZ.....a|n..!j&.g.Z.....-.....8.?.|z..nG...".2...O1U.....N.....SQ.6lSnG(.l....Ml ...5..!.....+....H.>..~..o`..W./.....E....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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\OR0WKIO1\eaMqCdNxIXjLc0ATep7tsFkfmSA.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2678
Entropy (8bit):	5.2826483006453255
Encrypted:	false
SSDEEP:	48:5sksiMwg1S0h195DlYt/5ZS/wAtKciZIgDa4V8ahSuf/Z/92zBDZDNJC0x0M:yklg1zbed3SBkdZYcZGVFNJCRM
MD5:	270D1E6437F036799637F0E1DFBDCAB5
SHA1:	5EDC39E2B6B1EF946F200282023DEDA21AC22DDE
SHA-256:	783AC9FA4590EB0F713A5BCB1E402A1CB0EE32BB06B3C7558043D9459F47956E
SHA-512:	10A5CE856D909C5C6618DE662DF1C21FA515D8B508938898E4EE64A70B61BE5F219F50917E4605BB57DB6825C925D37F01695A08A01A3C58E5194268B2F4DB3D
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/eaMqCdNxIXjLc0ATep7tsFkfmSA.gz.js
Preview:	var IPv6Tests;(function(n){function c(t){var r,c,o,l,f,s,i,a,v;try{if(y(),t==null||t.length==0)return;if(r=sj_cook.get(n.ipv6testcookie,n.ipv6testcrumb),r!=null&&r=="1"&&!u)return;if(c=sj_cook.get(n.ipv6testcookie,n.iptypecrumb),r!=null&&c&&u&&(o=Number(r),l=(new Date).getTime(),o!=NaN&&o>l))return;if(f=_d.getElementsByTagName("head")[0],!f)return;if(s="ipV6TestScript"+t,i=sj_ce("script",s),i.type="text/javascript",i.async=!0,i.onerror=function(){Log.Log("ipv6test","IPv6Test Dom_ "+t,"IPv6TestError",!1,"Error","JSONP call resulted in error.")},a=_ge(s),a&&f)return;f.insertBefore(i,f.firstChild);i.setAttribute("src",_w.location.protocol+"//"+t+".bing.com/ipv6test/test");e&&p();v=u?(new Date).getTime()+h:"1";sj_cook.set(n.ipv6testcookie,n.ipv6testcrumb,v.toString(),!1)}catch(w){Log.Log("ipv6test","Dom_ "+t,"IPv6TestError",!1,"Error","Failed to make JSONP call. Exception - "+w.message)}}function l(t){if(!t){Log.Log("ipv6test","IPv6TestResponseError","IPv6TestError",!1,"Error","Got null re

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\hqx6FcD0hjfzrON5oLgx2RMMD1s.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	443
Entropy (8bit):	4.86644754379557
Encrypted:	false
SSDEEP:	12:kdXCJAUQECJA5MeMJA561cnGfbs4Hbrk86fYXChdJAjU:8CJWECJKMeMJK61cuo47rk8WYMdJyU
MD5:	56583BD882D9571EC02FBDF69D854205
SHA1:	8DFF13B78F4CBCC482DC5C7FC1495390200C0B94

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\hqx6FcD0hjfzrON5oLgx2RMMD1s.gz[1].js	
SHA-256:	DF0089A92B304A88F35AA0117CF8647695659AAF68B38B1B7A72A7C53465E9C7
SHA-512:	418B3003B568F2FDB862035EE624CE93087861AEBB6680CDC0E0F1212297B64D30596EEF931B8C6E818292C4AB14C8C17FF0BAF9E58ED93392AD7A80621EBBE
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/hqx6FcD0hjfzrON5oLgx2RMMD1s.gz.js
Preview:	var OutlinePolyfil=function(){function n(){var n=this;this.attachHandlers=function(){n.attachHandlersForOutline()};this.attachHandlersForOutline=function(){addEventListener("keydown",n.onTabKey);addEventListener("mousedown",n.onMouseDown)};this.onTabKey=function(n){n.keyCode==9&&document.body.classList.add("tabbing")};this.onMouseDown=function(){document.body.classList.remove("tabbing")};this.attachHandlers()}return n}();new OutlinePolyfil

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\n1U5gwBiwMo7s-fWOh2kSe3Kils[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=5, xresolution=74, yresolution=82, resolutionunit=2, software=GIMP 2.10.8, datetime=2019:07:31 17:53:43], progressive, precision 8, 160x160, frames 3
Category:	downloaded
Size (bytes):	12094
Entropy (8bit):	7.886865463015066
Encrypted:	false
SSDEEP:	192:SiKi8QXz83TatNZ7rBakT+m47amRNj5y4zYOyuRHExmmjGjWddkuz4nicyktAtmR:SRi8083g7rBamzWNjPzguCxmmjGid60g
MD5:	05034EB84E5E7915CA36EB6FE59DFBA7
SHA1:	9F5539830062C0CA3BB3E7D63A1DA449EDCA8A5B
SHA-256:	9BEC2E05752C0699DB84352BB6E3DD4E5DAA927D32EC8123966F4A8FDF8B181A
SHA-512:	EB645D1FBB404B00D19C743C3F6F00597D91DE73EA2F02AE61AB76AFB13A913F68CB2419C205684CAD827D1369D8F76D9B7E709B8EF0AB05A86B305A7A5B708 9
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/n1U5gwBiwMo7s-fWOh2kSe3Kils.jpg
Preview:	.....JFIF.....H.H.....zExif..II*.....J.....R...(.....1.....Z...2.....f...z...H.....H.....GIMP 2.10.8.2019:07:31 17:53:43..... .....JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222.. ....."....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..8...R.Vf.|lcR.....sJ.#...1+..VR:b.b....8&*B.Qq.fj.6W50....`L.z..OrK_.+v..+..2....1.Q...K!.b..n.).A.j.s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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
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\OR0WKIO1\n_C4vBfAV3O9RfkGjfduaZoxjAs[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=5, xresolution=74, yresolution=82, resolutionunit=2, software=GIMP 2.10.8, datetime=2019:08:01 11:40:12], progressive, precision 8, 160x160, frames 3
Category:	downloaded
Size (bytes):	17171
Entropy (8bit):	7.923606790170532
Encrypted:	false
SSDEEP:	384:oYOT4bsa8uRaCLYIrdjf7xR346jojxR0WKHfoe:oYOT4Ya8uRnxT/346AhKHfoe
MD5:	D7AE018EA70FA15F5E5389E4F96AD768
SHA1:	9FF0B8BC17C05773BD45F9068DF76E699A318C0B
SHA-256:	A4F4A44961E03A073E3F351F296EC19C50005AA96360A9E5CEE50E0587738FBB
SHA-512:	FD5B341BECCBBE7C16065217BBCAF6DF2C44629DE778E1263FE6A071565718C920335DBA220FDDF8EB18ECBBF2BEBC698B03BCF555949CB3DD665752494714 06
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\n_C4vBfAV3O9RfkGjfduaZoxjAs[1].jpg	
IE Cache URL:	http://https://www.bing.com/rp/n_C4vBfAV3O9RfkGjfduaZoxjAs.jpg
Preview:	......JFIF.....H.H....(.Exif..II*.....J.....R...(.....1.....Z...2.....f...z...H.....H.....GIMP 2.10.8.2019:08:01 11:40:12..... .....(.....JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222.. ....."..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...3J8...D....m8P...\.L..c..%.4.R...@.iqJ.4.CCJ.o.....-.!...1.Q.LB...S.U~...iXw.1J(..b.o.b.zSsHb.@..(... .H:...M.O4.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\sTWC0LplwPyIP_jw8VjHps800ZQ.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	16386
Entropy (8bit):	5.2866519663601315
Encrypted:	false
SSDEEP:	384:+WLj/9N/zdUjP+c4QQKaK9JASETkyWJLhjO4YuiqRqNlRxW+:+u/P/zdUraOJhaShK1uiqR0T3
MD5:	44AD44162E25A1DB1F46F78B8ECFAD42
SHA1:	C63A0E7B132221D572A541F700601356627A98A4
SHA-256:	5AE500A4737BE7B187EEA99AAB81CF3D4796D23550F7C5349DE2430E6624918D
SHA-512:	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\OR0WKIO1\swyt_VnIjJDWZW5KEq7a8l_1AEw.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2298
Entropy (8bit):	5.34865319631632
Encrypted:	false
SSDEEP:	48:KWEkTScZVcMBOwXhzwBi88RnX8ec0T39B8onA008xG9FLCx3w0S5xJ:KWEkTDZVXpR0BiXjTtB8mA0zxWsx3PG/
MD5:	A8D7D1B3681590980B2D7480906078DB
SHA1:	C9A7A400DB1EBAD4DCA028546EE5F5B2EF4136BD
SHA-256:	1390485DC88B6230389D9C95232A3710BF38D47271708A279B12D7E68E43F649
SHA-512:	710D31EFD76614EC4C94888E2FCC49ABAB50EF406FC0F1C5C10D8AA21D4E9F349DE78068B2BAFE495C074AB4E6EC0A5D44EB5506B2D79C78707A23C1D8206664
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/swyt_VnIjJDWZW5KEq7a8l_1AEw.gz.js
Preview:	var Bnp=Bnp||{};Bnp.Global=Bnp.Global||{};Bnp.Version="1";Bnp.Partner=Bnp.Partner||function(){function u(n){sj_evt.fire("onBnpRender",n)}function i(n){var r=r||{};if(typeof r.stringify=="function")return r.stringify(n);var o=typeof n,u=n&&n.constructor==Array,f=[],e,t;if(o!="object"||n==null)return o=="string"?""+n+"":String(n);for(e in n)t=n[e],t&&t.constructor!=Function&&(u?f.push(i(t)):f.push(""+e+":"+i(t)));return(u?"[":"{")+String(f)+(u?"]":"}")}function o(n){for(var r=[],u=n.getElementsByTagName("script"),t,i;u.length;)t=u[0],i=sj_ce("script"),t.src?i.src=t.src:t.text&&(i.text=t.text),i.type=t.type,t.parentNode.removeChild(t),r.push(i);return r}function s(n){for(var t=0;t<n.length;t++)f(n[t])}function f(n){t=t||_d.getElementsByTagName("head")[0];t.appendChild(n)}function h(n){for(var t,i=0;i<n.length;i++)t=sj_ce("style"),t.type="text/css",t.textContent!=undefined?t.textContent=n[i]:t.styleSheet.cssText=n[i],f(t)}function c(){sj_evt.fire("onPopTR")}var n="dhplink",t,e=2500,r=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\th[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 1920x1080, frames 3
Category:	downloaded
Size (bytes):	344983
Entropy (8bit):	7.987666031914428
Encrypted:	false
SSDEEP:	6144:uhr6bFSzjuZdOJGR0u6FY7Kq1u9ktnbQ9uJ4g2FUXoIQc1tYJsDr0j:AwFEjSOJbuYphkZQ9uJX22TQc1qJwa
MD5:	DDCE5ED235CCBFFDA3F3735F75F80C0F
SHA1:	F266C24FA6F01459F51C97ADB00523BD214C653C
SHA-256:	78EB4A3213EBE7BB95F87D206AE29064D514628E6A430334D0E13756AA131DE5
SHA-512:	A0C70871BC52467524A0107F09B93C1BE11FFBD9CF68E1F3C567F97B0F810AA5B0CEE584AE1BA720F4A0B30F42E4290A06E99B9EA640437B0DABF158F2DB0625
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?id=OHR.Olympics125_ROW9889344454_1920x1080.jpg&rf=LaDigue_1920x1080.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\th[1].jpg	
Preview:	......JFIF.....C..... "" .,,,.3333333333...C..... ....## ##,,),,3333333333.....8...."..... S..... ....!1A.."Q2aq..B...#R...b.3r....$C.....4Scs..%DT...u.5t..... B.....!..1AQ."aq.2.....BR..#br.$34..C....Ss...c.....?.#...9.%qx..fL.Z..+p.....+...X .2m...,..X.<..W...}Dk.\J....f9.~.....b.../.7C&.V.Y.9`.|.rV0'>.9.....3._>.6.@...ML-...+].Q.....]....'>.`e..W>.9.....|.d...>.9..VJ.Es./.%e....,..y.7.....l.....g.4.3g)..d.99Bk....+r. :e$.ca.SH.|.....m...}.YRO9...j.vd..9V..5..@e...{.<hA...:.....9K#.....q.H...`....q>NiF=.[..2C.8X...*.....L(.{.....s.3.W.!....{^..'..~....9.!..^A.y...1.A..[.....l!a....i ..)L.D.D.8#.{../.0.\.M. .r..qg3...t.N..^....L.I3'.....eQ.`3{.....Yh...sK...k..I...m.o.t^%e...O..e&a.....9..v.x....&.E!.e..p.....n.UQ.x$S\.....1}DqH

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\th[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	6319
Entropy (8bit):	7.921601448672384
Encrypted:	false
SSDEEP:	96:pPE3Um+CGqdS0RiboPJ5pa8ao3aO+MmlFKzJC1u/b8D8z2Lu0J+Vwe7qC:pPWrpU+5Rao3/LmuzJCM/bzgAz
MD5:	35639C3C895B57D5E4B5F764ABE5D940
SHA1:	269D5DE5F01924ADF9665A9F4D163EA553794BAA
SHA-256:	EA18037D4EB9771263CCA340B2AD31DA0CA807DAE7CDF8FD437266A853DE3D00
SHA-512:	6EB07EF59332D95985DA086B8FC1CA8A762D31CC6FCC14418C736CF211FB5B06381F876BF77C334C7140800BA5DBDEB1EAF07A401E47F0C4ABDEAD2D836389 2
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkJLx.img&ehk=ab4NFwKPiOUcoMjMzCCRK%2fouai5ROn4RlXwrt3nrHLY%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....,.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====..... ....."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....L..]..:0..!t3<.....?x}k....tEgv..")ff'.....s.....Q..=...S....W.z....x.....X.....}..Z.....[}....\.....>....X(6i*.lbi..u[..P...O...y..E..l...%..:....Qwu.?...qz..u._ r.|.B.....M(..$.p...).9.z....zW.....[.....?C.m...dE..(.h.M.....v<..q..S6Yn...G.<....T.>V..|T.O]>.....-.....j.?L..X....S.@.H...L...P".Y..TT...~O..!..n....ecp.n..H...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\th[3].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	4579
Entropy (8bit):	7.899738415633208
Encrypted:	false
SSDEEP:	96:pPElQIszgVi+8yJg1On37lfYKgsaU4AzO/wVie:pPk50gd8ysW5QKgizce
MD5:	6252E142AFB55FA1C5DD093059E5B784
SHA1:	FA2DEDFB97B7BF7B2D1052EA4B0DEC214E4217A1
SHA-256:	24461B5094C1DC8AA9F6741AD78006FF35954478933E003E2CD036EA8E303EA4
SHA-512:	A6156F1C962CE251B79C86F5A5B5BBA8C3D8C1060251CD69365C650D5BF2480ED14A6F36CFF4235BB0E53DC15903086CF901891B2DEEC050271A851D88C3DE/
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fket7.img&ehk=x1iCxRdz8nKwKjWtFCBaxEx1tovE7Q0NcYc3bmTeH%2fl%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....,.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====..... ....."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..f..$H.."(.f'..rk..9.....B<...9.c.:...E,.....=...w.....,_h.....yttW=.....tr..>l0..+.fE.,z..s..js.....5,.....i.....+.Cm=.3Sj.6.|.r...>.G.....W.Z.]){..i[..&.C...,.*A. ..s.u.....s.S.>ni..t.;....OH..i.3N.R.[..2..7..*.#.}SP..O.X@.....zt98.YzR..2..9.`Y..r..ZN.,..+9Tp.....C.cS.>.PT..X.....S..8S..moJV..<.>..Z.U.).7ZV..!..h.0.S.\..eX5k)..Gp.O....J..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\th[4].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	2724
Entropy (8bit):	7.802617302004863
Encrypted:	false
SSDEEP:	48:pyYcuERASOUUUoZPAQUPWFxscd6Fy2YCY43L5Xu2yllZzixFrn363zsIrOotgVr:pPE7ziZIQ7xscCyBIL5u2yldK3wYStgp
MD5:	28EB07FE60190EFB31CB18CFD3D7A18E
SHA1:	4AD266DDF9B415DFEA6AB163AEEAAB8F2FEB3D25
SHA-256:	89765095BB7B7DFA92CE3D9F7592BA8F776A68B3C603137C4AF2A4CDF73A8A91
SHA-512:	0E388A8F601FF92C0114409E63D54EDD20DABBC1A0F850D27A7F193C41A876A9E2C45B48926B71BB76453B73292D1C7BE8EC3A8E9BE100D9AE8B24D796F3898 B
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkeHo.img&ehk=87%2bfrmCNlDAG6dOQDPGJoEnt2SWJJyVXRhRVoIJ02S0%3d&w=150&h=150&c=8&rs=2&pid=WP0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\th[4].jpg	
Preview:	......JFIF.....``.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====.. .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....<P.8.x\.7=.....7:#H.m(Z.o...j...Dai.).i.}.\.4....{R...sUH.V.....:D.i.jr..I.....SC.q.T.Q...BE4.eN...FLn.dg.../..p6.....O.!....;.z...S... ..!O.|."....Ja#.4..QI ...5V.....5.gT)...I.J#.<E..77..5.<...0`6..@C.V..{R.%Yw....U+..g..P....k.t..sz..d_*1.f.R....cU..+.d.i.Yj2.m..e.5I..A.8U..6...{"....\..i.sW.G$P.B..c.i..g....U{....M..H.....y'..&6B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\th[5].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	4858
Entropy (8bit):	7.912860451432217
Encrypted:	false
SSDEEP:	96:pPE/rJtrOaBegYjEZcV2CWr45p5VrbFU4/PbFI+tMpg:pPYKaBeXE6d59bLui
MD5:	C27EAAD7FDCAD067348EB8426A6643DD
SHA1:	D5362D86359F58F1F08EBC9E9F7627F61CB70909
SHA-256:	20EA77BAF0828E450BB7EB0895759B7C760D1F4C00B1EF5366F91B2F23B30429
SHA-512:	AF46A7A9FAEF467FBBA40194C4B8E6A57EDF476ACC10CBEE4CADF87E8CFFA5DBCCB6EC6601944724148F59E8EBCB317442F88BE272657EC4A9EDC841B984F BD2
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkGpp.img&ehk=EoXsvHvTz25OeDlk8%2f1AsQ0JRbPiNyy0iD13c2N9OGI%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....``.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====.. .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..%8&jP....p..u..p"..z....e.....`.1....:.....J.O3.....k.....6I.J0..1..&K..(P...GS[..b.(."....`zT.....I...3..}g<ig.M.r....~5.....[.....sz.f^.....(^Cg..{...1..... n1.`..A.*.I....m+;Gx.....3..q[..!.p.....G..>VrU.+..).*..iZ.9lU)L)V.SJS$.R.V...2S..J.E...]...sEJR..:5L... ....)..@..s]|i..W..d7.<k.v.=z.....p.=l..,L.]....4...L..c.Q....j..}.%.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\th[6].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	5038
Entropy (8bit):	7.913300499070733
Encrypted:	false
SSDEEP:	96:pPEvzuSDKiT+ERod8yBN0X/HmlRJJ+Fn8h3fzh+LZvwk:pPOCSmHhW/H4JJ+F8xzh+L9wk
MD5:	B4253CC44B582EBE891CBCDF0EF5CA8B
SHA1:	2D179CB4C761077F9EFB53625FE0B34D01AE3107
SHA-256:	9358906D6A9154E881A96AA4E9EDED3CCFDF3DC87B1B922B8FC4C09B970130F5
SHA-512:	6D3EA094D383E370E85CBDD445B76D8B2986B3F175145F8DB93112A63E48DF8FA1877BBFD25C2CA73CE66B2C1DECF7FAB01D9556855CF9DD1F9462D4432F60 B
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1flcl7.img&ehk=n4zxNzUaGmaWvZYudQOxjiEm8O7nfdAvG5P6LGtz8zo%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....,.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====.. .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..(...).C$..$gbp..z=.P..`Tz...i.&..+nO._..f7'.....:.....[..zf..a..E.U.(...(...(...(...(...(.6v.....!..V.k.@.....N...>...Rxc.7:.i.....#.cz..k.4..[i6...bL1c...../.8./.Iob .D+....#,.s..O.I..U7.....z|.i2m.Y...[..j.....Xjodp'HXG..sw>.kJ...Fv2..(..z...D.9L.....b..-./..'....U....t..:}...DV-.u....>u..y...b...Xn.)' ..:.....<>t.e..0...U....=.oN..f...8.(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\th[7].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	5777
Entropy (8bit):	7.917920871216737
Encrypted:	false
SSDEEP:	96:pPEQBGjpz1df7dAJrDp5OiC9PchAeKBc9VSwpCcGpZcU1DwGO1pHRsKdDcn:pPTBGjlrf7dNchnrCnZcUwG4Rldon
MD5:	7D10F16EA455E49470853BE05415E27E
SHA1:	0370FE7D24274A9A5909355C042EBBF9E795FD85
SHA-256:	1DB14FB96D4E49265DEFB60E98BD6C39A2724B1EBC21D50E0F2E60F3859EE93A
SHA-512:	DF233159BC504BA5C8D8759AE631A2D5CE9AB48060EDC84EEF2674749AEE1D5E0A3B5BD5AE8EF3F54FDFBBD1F7FE0B9D26FD1FC99593DAC78396EE2209CE1 B0C
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\th[7].jpg	
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1flksC.img&ehk=H0FCoWHkkRHx9dwEmzqiKOqgx9bfKAuVCxCQfuDoLvw%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....,.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)==========..."..}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....;@..^H[~O.=..I.5.s.....8.....%'=..Hd.q..?.W'..... .;..J$...=.E$.P1.h../..7.z.....ZxF.....f1...R.~...i\v!..... .>...u!...9.....\<.I..A....8.....#....-.....h..\|.#tcV..e....1Q.A..W].qV..*..B.i$.z7...Kz.(..l7.#....T?3...o7..H..c(..O..qYF-d.w.\.#.P...y..Hn&~J.S.c5j..6..c....b...N6.L..F.=..M.(.dw..2....f.ce;GC..W*.x|.....*5.....4....v!.c.t 4.+7.9.5".J

C:\Users\user\AppData\Local\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):	4.547386139474471
Encrypted:	false
SSDEEP:	3:oVXU15FdXqW6IR98JOGXnE15FdXqW6mn:o9U7Fd1R9qE7FdZ
MD5:	F2D80931FCBF997039DD580CA825951D
SHA1:	FD8700AE5A6EC0B3EA3CC265A572251CEE9195F7
SHA-256:	37E874C9732FF741888E1B377BE726977CFD23D295080C9FFB087617AC499285
SHA-512:	E886C8D9579310FDB888CA6B5BEA69F2FAA1694D8FF8F2B5E8F68207AD53E6C5144708C96856DA3CC23D7A1F0A9C38BCBEFCF284FF1EB7776F98DF92384371A
Malicious:	false
Preview:	[2021/04/06 09:52:25.838] Latest deploy version: ..[2021/04/06 09:52:25.838] 11.211.2 ..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.969255920414703
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:	gg.gif.dll
File size:	103055
MD5:	75ffb2cb4faff68f2649a4f6f16840d9
SHA1:	543803cbfad26ff1e538e0843161ef6729ff3a85
SHA256:	db9ede8dfbecb23b804cd592eeb7500e397ade3bc1fa01551a912ae572cda8b3
SHA512:	4fd79ea6b6a6d6cb36287e6a2bd4f08ca8881f3ad82ca37af771701fa4ec7d7d69f68b64723728ea6241beb8fddffb8ab6ca1057d1069783bcfac16d9ea0d19d
SSDEEP:	1536:DWKaY5Se9WnVI78XvnoxJasJvRHKmyGDvDk0Rt9Y56l5ZMpvV05o9OX5xPw8:DWa0eQnVI7qCqZGDvDk4wol5w0EU
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._W...6e..6e..6e..)v..6e...w..6e.Rich.6e.....PE..L.....f`.....!.....Z.....`.....p.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10006099

General

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

Entrypoint Preview

Instruction
push ebx
push ebx
and dword ptr [esp], 00000000h
add dword ptr [esp], ebp
mov ebp, esp
add esp, FFFFFFF8h
push esi
mov dword ptr [esp], FFFF0000h
call 00007FA3FCBEC6C0h
push ecx
add dword ptr [esp], 00000247h
sub dword ptr [esp], ecx
push ecx
mov dword ptr [esp], 00005267h
call 00007FA3FCBE9069h
push esi
mov esi, eax
or esi, eax
mov eax, esi
pop esi
jne 00007FA3FCBEE162h
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]

Instruction
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 00007FA3FCBEE13Eh
add dword ptr [ebx+004180F7h], ebx
add dword ptr [ebx+00418633h], ebx
mov dword ptr [ebp-04h], edx
sub edx, edx
xor edx, dword ptr [ebx+004180F7h]
mov esi, edx
mov edx, dword ptr [ebp-04h]
push edi
xor edi, dword ptr [esp]
xor edi, dword ptr [ebx+0041856Bh]
and ecx, 00000000h
or ecx, edi
pop edi
cld
rep movsb
push ebx
mov dword ptr [eax+eax], 00000000h

Data Directories

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

Sections

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

Imports

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

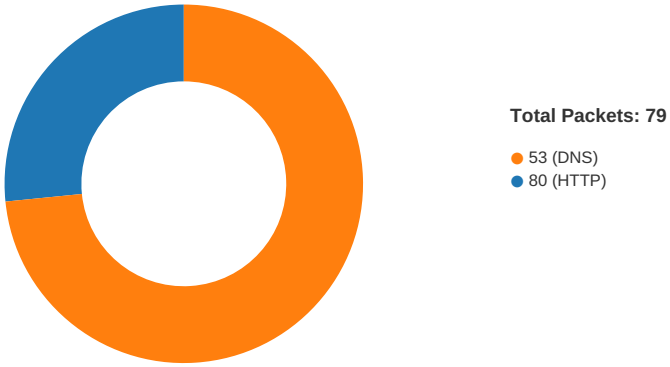
DLL	Import
comctl32.dll	DPA_Sort

Exports

Name	Ordinal	Address
StartService	1	0x1000b959

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 09:52:26.566813946 CEST	49783	80	192.168.2.4	185.243.114.196
Apr 6, 2021 09:52:26.567709923 CEST	49782	80	192.168.2.4	185.243.114.196
Apr 6, 2021 09:52:27.456983089 CEST	49784	80	192.168.2.4	185.243.114.196
Apr 6, 2021 09:52:27.457223892 CEST	49785	80	192.168.2.4	185.243.114.196
Apr 6, 2021 09:52:27.571407080 CEST	49782	80	192.168.2.4	185.243.114.196
Apr 6, 2021 09:52:27.571541071 CEST	49783	80	192.168.2.4	185.243.114.196
Apr 6, 2021 09:52:28.462287903 CEST	49785	80	192.168.2.4	185.243.114.196
Apr 6, 2021 09:52:28.462421894 CEST	49784	80	192.168.2.4	185.243.114.196
Apr 6, 2021 09:52:29.571890116 CEST	49782	80	192.168.2.4	185.243.114.196
Apr 6, 2021 09:52:29.587296009 CEST	49783	80	192.168.2.4	185.243.114.196
Apr 6, 2021 09:52:30.462409019 CEST	49784	80	192.168.2.4	185.243.114.196
Apr 6, 2021 09:52:30.462423086 CEST	49785	80	192.168.2.4	185.243.114.196
Apr 6, 2021 09:52:33.589245081 CEST	49787	80	192.168.2.4	185.243.114.196
Apr 6, 2021 09:52:34.464323044 CEST	49788	80	192.168.2.4	185.243.114.196
Apr 6, 2021 09:52:34.479861975 CEST	49789	80	192.168.2.4	185.243.114.196
Apr 6, 2021 09:52:34.587610960 CEST	49787	80	192.168.2.4	185.243.114.196
Apr 6, 2021 09:52:35.462898970 CEST	49788	80	192.168.2.4	185.243.114.196
Apr 6, 2021 09:52:35.494090080 CEST	49789	80	192.168.2.4	185.243.114.196
Apr 6, 2021 09:52:36.587888002 CEST	49787	80	192.168.2.4	185.243.114.196
Apr 6, 2021 09:52:37.478543997 CEST	49788	80	192.168.2.4	185.243.114.196
Apr 6, 2021 09:52:37.494900942 CEST	49789	80	192.168.2.4	185.243.114.196

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 09:50:49.906055927 CEST	59123	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:50:49.961967945 CEST	53	59123	8.8.8.8	192.168.2.4
Apr 6, 2021 09:50:52.211869001 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:50:52.260478020 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 6, 2021 09:50:52.870242119 CEST	49714	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 09:50:52.930224895 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 6, 2021 09:50:55.048005104 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:50:55.093986988 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:20.269418001 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:20.318228960 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:20.756989956 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:20.804409027 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:21.181500912 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:21.246119022 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:22.169919968 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:22.216470957 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:23.136452913 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:23.184880972 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:24.204544067 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:24.251733065 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:25.127532959 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:25.177489042 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:25.725207090 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:25.784171104 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:31.996843100 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:32.046298027 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:32.868232965 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:32.914139032 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:35.110240936 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:35.164710999 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:36.026846886 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:36.075781107 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:39.528892040 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:39.585572004 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:41.057960033 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:41.186247110 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:41.375370979 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:41.421170950 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:41.505682945 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:41.551507950 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:41.690042973 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:41.752110958 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:41.768003941 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:41.831078053 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:42.120459080 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:42.174755096 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:42.395884037 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:42.544260025 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:42.632412910 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:42.678339958 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:42.771600962 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:42.830657959 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:42.897424936 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:42.943372011 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:42.989135027 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:43.043612003 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:43.155049086 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:43.212351084 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:43.968080044 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:44.022542953 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:44.147030115 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:44.195888996 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:44.695607901 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:44.750025034 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:45.215624094 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:45.272998095 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:45.650223017 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:45.707933903 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:46.174978018 CEST	50183	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 09:51:46.178119898 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:46.226866961 CEST	53	61531	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:46.244849920 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:46.597022057 CEST	49228	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:46.644252062 CEST	53	49228	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:47.062550068 CEST	59794	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:47.116751909 CEST	53	59794	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:47.640690088 CEST	55916	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:47.737066984 CEST	53	55916	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:53.992728949 CEST	52752	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:54.049031973 CEST	53	52752	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:54.907463074 CEST	60542	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:54.956118107 CEST	53	60542	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:56.297413111 CEST	60689	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:56.344780922 CEST	53	60689	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:57.511923075 CEST	64206	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:57.567507029 CEST	53	64206	8.8.8.8	192.168.2.4
Apr 6, 2021 09:51:59.070137978 CEST	50904	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:51:59.115982056 CEST	53	50904	8.8.8.8	192.168.2.4
Apr 6, 2021 09:52:09.446861029 CEST	57525	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:52:09.492707014 CEST	53	57525	8.8.8.8	192.168.2.4
Apr 6, 2021 09:52:10.445367098 CEST	57525	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:52:10.491389990 CEST	53	57525	8.8.8.8	192.168.2.4
Apr 6, 2021 09:52:11.462462902 CEST	57525	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:52:11.508475065 CEST	53	57525	8.8.8.8	192.168.2.4
Apr 6, 2021 09:52:13.461791039 CEST	57525	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:52:13.507920027 CEST	53	57525	8.8.8.8	192.168.2.4
Apr 6, 2021 09:52:17.477314949 CEST	57525	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:52:17.523367882 CEST	53	57525	8.8.8.8	192.168.2.4
Apr 6, 2021 09:52:25.379019976 CEST	53814	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:52:25.439323902 CEST	53	53814	8.8.8.8	192.168.2.4
Apr 6, 2021 09:52:26.470719099 CEST	53418	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:52:26.529123068 CEST	53	53418	8.8.8.8	192.168.2.4
Apr 6, 2021 09:52:27.387382984 CEST	62833	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:52:27.442384958 CEST	53	62833	8.8.8.8	192.168.2.4
Apr 6, 2021 09:52:31.875679016 CEST	59260	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:52:31.925056934 CEST	53	59260	8.8.8.8	192.168.2.4
Apr 6, 2021 09:52:40.614671946 CEST	49944	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:52:40.668962002 CEST	53	49944	8.8.8.8	192.168.2.4
Apr 6, 2021 09:52:41.501399040 CEST	63300	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:52:41.558743000 CEST	53	63300	8.8.8.8	192.168.2.4
Apr 6, 2021 09:53:02.527239084 CEST	61449	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:53:02.583650112 CEST	53	61449	8.8.8.8	192.168.2.4
Apr 6, 2021 09:53:03.407155037 CEST	51275	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:53:03.464885950 CEST	53	51275	8.8.8.8	192.168.2.4
Apr 6, 2021 09:53:03.506134987 CEST	63492	53	192.168.2.4	8.8.8.8
Apr 6, 2021 09:53:03.573776960 CEST	53	63492	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 6, 2021 09:51:42.632412910 CEST	192.168.2.4	8.8.8.8	0x962	Standard query (0)	login.micr osoftonline.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:51:42.897424936 CEST	192.168.2.4	8.8.8.8	0x6297	Standard query (0)	login.micr osoftonline.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:52:26.470719099 CEST	192.168.2.4	8.8.8.8	0x839a	Standard query (0)	under17.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:52:27.387382984 CEST	192.168.2.4	8.8.8.8	0x5e20	Standard query (0)	under17.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:52:40.614671946 CEST	192.168.2.4	8.8.8.8	0xad6b	Standard query (0)	under17.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:52:41.501399040 CEST	192.168.2.4	8.8.8.8	0x5fdc	Standard query (0)	under17.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:53:03.407155037 CEST	192.168.2.4	8.8.8.8	0x5ecf	Standard query (0)	urs-world.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 6, 2021 09:53:03.506134987 CEST	192.168.2.4	8.8.8.8	0xa337	Standard query (0)	urs-world.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 6, 2021 09:51:42.678339958 CEST	8.8.8.8	192.168.2.4	0x962	No error (0)	login.microsoftonline.com	a.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 09:51:42.678339958 CEST	8.8.8.8	192.168.2.4	0x962	No error (0)	a.privatelink.msidentity.com	prda.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 09:51:42.678339958 CEST	8.8.8.8	192.168.2.4	0x962	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 09:51:42.830657959 CEST	8.8.8.8	192.168.2.4	0x65c4	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 09:51:42.943372011 CEST	8.8.8.8	192.168.2.4	0x6297	No error (0)	login.microsoftonline.com	a.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 09:51:42.943372011 CEST	8.8.8.8	192.168.2.4	0x6297	No error (0)	a.privatelink.msidentity.com	prda.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 09:51:42.943372011 CEST	8.8.8.8	192.168.2.4	0x6297	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 09:51:43.043612003 CEST	8.8.8.8	192.168.2.4	0xcb0d	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 09:52:26.529123068 CEST	8.8.8.8	192.168.2.4	0x839a	No error (0)	under17.com		185.243.114.196	A (IP address)	IN (0x0001)
Apr 6, 2021 09:52:27.442384958 CEST	8.8.8.8	192.168.2.4	0x5e20	No error (0)	under17.com		185.243.114.196	A (IP address)	IN (0x0001)
Apr 6, 2021 09:52:40.668962002 CEST	8.8.8.8	192.168.2.4	0xad6b	Server failure (2)	under17.com	none	none	A (IP address)	IN (0x0001)
Apr 6, 2021 09:52:41.558743000 CEST	8.8.8.8	192.168.2.4	0x5fdc	No error (0)	under17.com		185.243.114.196	A (IP address)	IN (0x0001)
Apr 6, 2021 09:53:03.464885950 CEST	8.8.8.8	192.168.2.4	0x5ecf	No error (0)	urs-world.com		185.186.244.95	A (IP address)	IN (0x0001)
Apr 6, 2021 09:53:03.573776960 CEST	8.8.8.8	192.168.2.4	0xa337	No error (0)	urs-world.com		185.186.244.95	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

- loaddll32.exe
- cmd.exe
- rundll32.exe
- rundll32.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6768 Parent PID: 6020

General

Start time:	09:50:57
Start date:	06/04/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\gg.gif.dll'
Imagebase:	0x1050000
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_1, Description: Yara detected Ursnif, Source: 00000000.00000002.922918490.0000000001020000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.797626012.00000000037EB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.797603385.00000000037EB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.797550182.00000000037EB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.797787648.00000000037EB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.797669563.00000000037EB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.797658293.00000000037EB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.878138434.00000000036ED000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.923843062.00000000035EF000.00000004.00000040.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: 6776 Parent PID: 6768

General

Start time:	09:50:57
Start date:	06/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\gg.gif.dll',#1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6784 Parent PID: 6768

General

Start time:	09:50:57
Start date:	06/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\gg.gif.dll,StartService
Imagebase:	0xe0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.684429763.0000000002FB0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6796 Parent PID: 6776

General

Start time:	09:50:57
Start date:	06/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\gg.gif.dll',#1

Imagebase:	0xe0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.796910446.000000000507B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.796966176.000000000507B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.924347640.0000000004E7F000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.796946194.000000000507B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.796993950.000000000507B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.923540871.0000000002C70000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.876439503.0000000004F7D000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.796929617.000000000507B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.796879072.000000000507B000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 7104 Parent PID: 800

General

Start time:	09:51:38
Start date:	06/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff60c330000
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: 64 Parent PID: 7104

General

Start time:	09:51:39
Start date:	06/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7104 CREDAT:17410 /prefetch:2
Imagebase:	0x860000
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: 4732 Parent PID: 7104

General

Start time:	09:51:41
Start date:	06/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7104 CREDAT:82948 /prefetch:2
Imagebase:	0x860000
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: 4864 Parent PID: 800

General

Start time:	09:52:24
Start date:	06/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff60c330000
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: 6196 Parent PID: 4864

General

Start time:	09:52:25
Start date:	06/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4864 CREDAT:17410 /prefetch:2
Imagebase:	0x860000
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: 7112 Parent PID: 4864

General

Start time:	09:52:26
Start date:	06/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4864 CREDAT:17414 /prefetch:2
Imagebase:	0x860000
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: 1364 Parent PID: 800

General

Start time:	09:53:01
Start date:	06/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff60c330000
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

Analysis Process: iexplore.exe PID: 6152 Parent PID: 1364

General

Start time:	09:53:02
Start date:	06/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1364 CREDAT:17410 /prefetch:2
Imagebase:	0x860000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis