ID: 381725
Sample Name: swlsGbeQwT.dll
Cookbook: default.jbs
Time: 16:00:51
Date: 04/04/2021
Version: 31.0.0 Emerald

Table of Contents

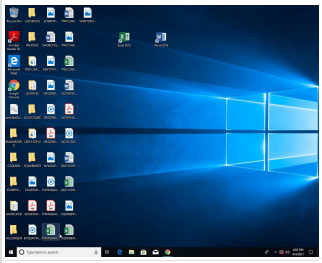
Analysis Report swlsGbeQwT.dll

Overview

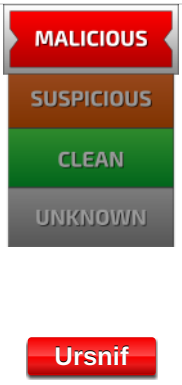
General Information

Sample Name:	swlsGbeQwT.dll
Analysis ID:	381725
MD5:	bedfac54b06b97b.
SHA1:	e238b2b47e1ccb..
SHA256:	22682ac6f8c4847..
Tags:	dll Gozi ISFB Ursnif
Infos:	

Most interesting Screenshot:



Detection



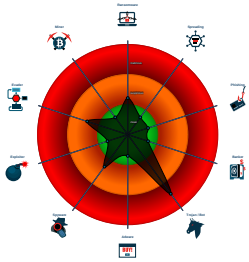
Ursnif

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6104 cmdline: loaddll32.exe 'C:\Users\user\Desktop\swlsGbeQwT.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 4832 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\swlsGbeQwT.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 3512 cmdline: rundll32.exe 'C:\Users\user\Desktop\swlsGbeQwT.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5076 cmdline: rundll32.exe C:\Users\user\Desktop\swlsGbeQwT.dll,StartService MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 6320 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6392 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6320 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 5316 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5340 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5316 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5736 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5316 CREDAT:17416 /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
00000005.00000003.332207803.0000000005AE8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000002.228615251.0000000001180000.00000004.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000001.00000003.283968924.0000000003138000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.283941629.0000000003138000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.283743972.0000000003138000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 18 entries

Unpacked PEs

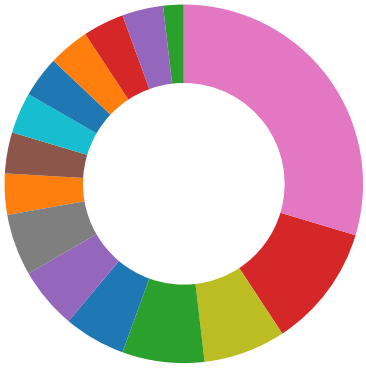
Source	Rule	Description	Author	Strings
4.2.rundll32.exe.1180000.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.2.loaddll32.exe.9c0000.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
5.2.rundll32.exe.3570000.3.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
5.2.rundll32.exe.10000000.5.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.2.loaddll32.exe.10000000.4.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Compliance
- Spreading



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

Click to jump to signature section

AV Detection:

Found malware configuration

Machine Learning detection for sample

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

Yara detected Ursnif

System Summary:

Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

Yara detected Ursnif

Remote Access Functionality:

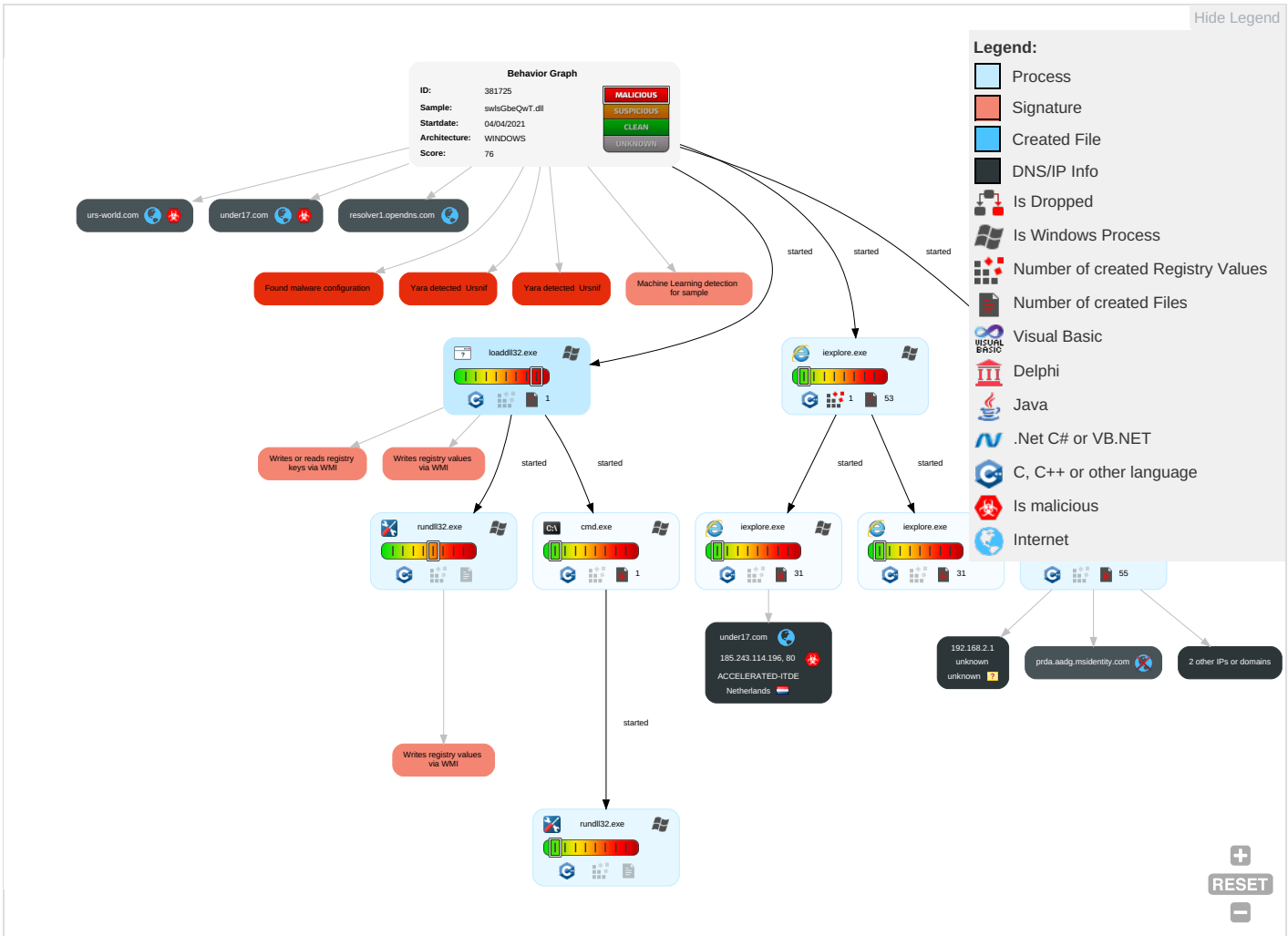
Yara detected Ursnif

Yara detected Ursnif

Mitre Att&ck Matrix

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

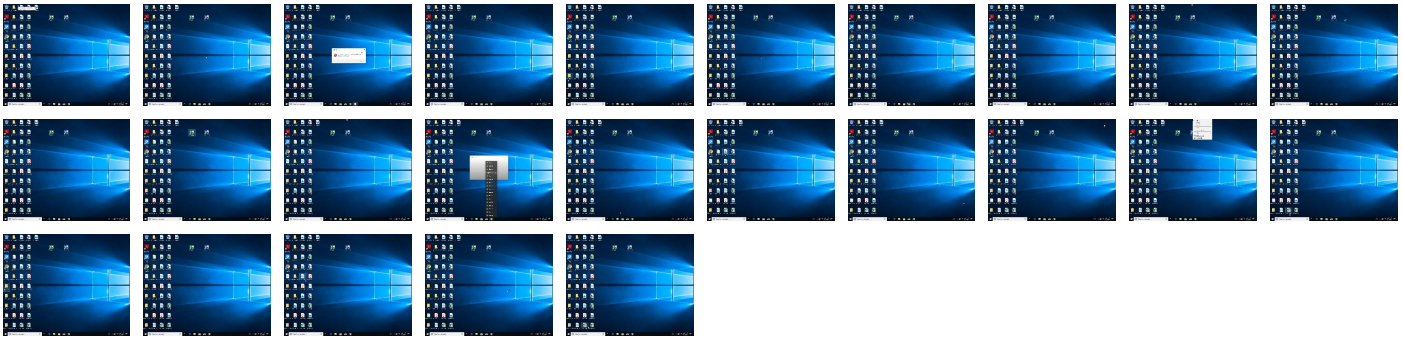
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
swIsGbeQwT.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.loaddll32.exe.a10000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
5.2.rundll32.exe.10000000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
5.2.rundll32.exe.ff0000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
1.2.loaddll32.exe.10000000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://urs-world.com/joomla/nyEGAUlxBMi/vJvW_2B31g3fIm/PJCeDCcMkYuKm3mBUGX2v/CaL9euzPRyB3Opxa/glJ_2B	0%	Avira URL Cloud	safe	
http://under17.com/joomla/4GzHZlWwziXisjjV671v1LT/84UlNg6ksC/Tggq4HFqFymyDjTMV/yfv7eGSUkzcX/52ysYFgN	0%	Avira URL Cloud	safe	
http://urs-world.com/joomla/nyEGAUlxBMi/vJvW_2B31g3fIm/PJCeDCcMkYuKm3mBUGX2v/CaL9euzPRyB3Opxa/g	0%	Avira URL Cloud	safe	
http://urs-world.com/joomla/LeY03GyFH8M9ux9Q/fhlrqhT7AEWHy5S/Gj6LLiVr5gZ24pcdoa/r9hh9gZTx/jUFCXHTg6g	0%	Avira URL Cloud	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://urs-world.com/joomlaaL9euzPRyB3Opxa/glJ_2BkxmWXAk4B/fa_2B_2FtCKRxglTM9/4omZ9P4fz/YwGhMR3ktfTd	0%	Avira URL Cloud	safe	
http://under17.com/joomla/bY332Z6nIw/mpCJzusDxBf4026z_/2BrGN0t7fT0r/o1u_2FGT8iB/giLHX9xa5y4nT5/E4muy	0%	Avira URL Cloud	safe	
http://under17.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

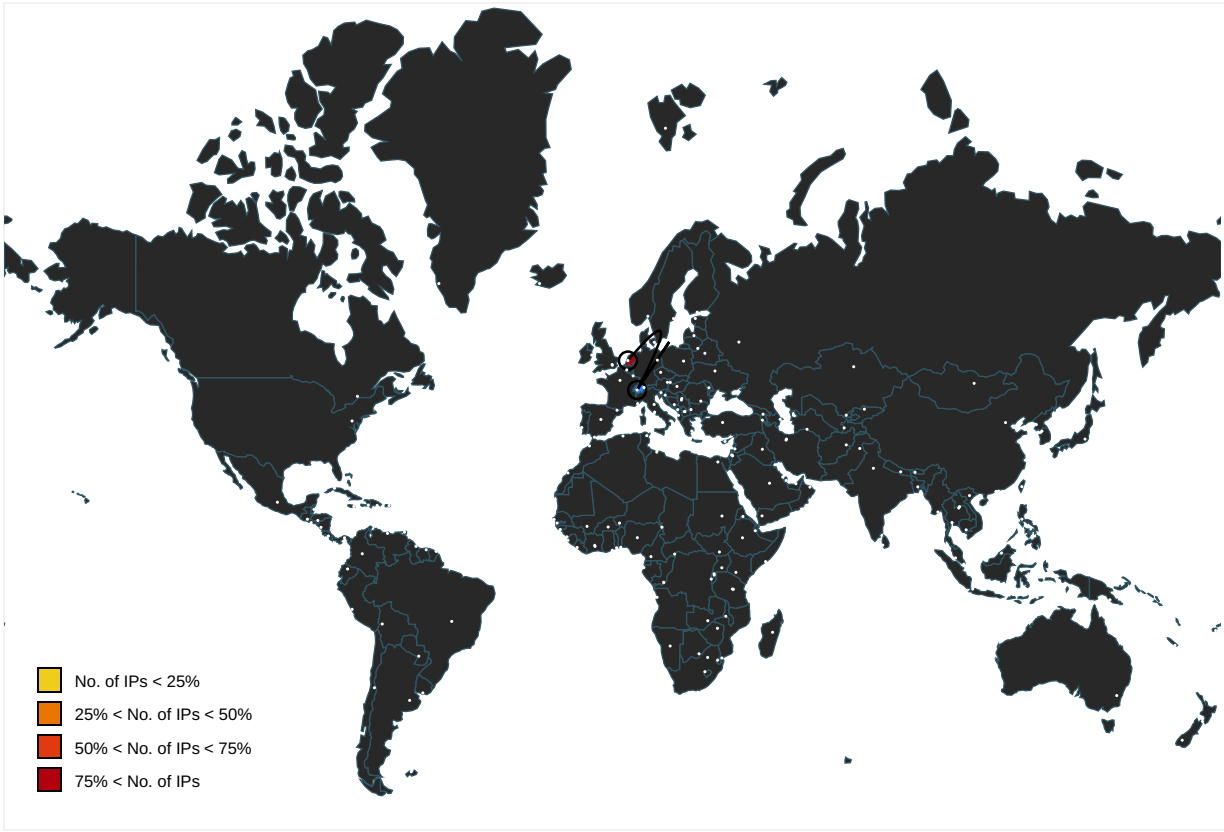
Name	IP	Active	Malicious	Antivirus Detection	Reputation
urs-world.com	185.186.244.95	true	true		unknown
under17.com	185.243.114.196	true	true		unknown
resolver1.opendns.com	208.67.222.222	true	false		high
login.microsoftonline.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://urs-world.com/joomla/nyEGAUlxBMi/vJvW_2B31g3fIm/PJCeDCcMkYuKm3mBUGX2v/CaL9euzPRyB3Opxa/glJ_2B	loaddll32.exe, 00000001.00000002.462447224.0000000000A2B000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://under17.com/joomla/4GzHZlWwziXisjjV671v1LT/84UlNg6ksC/Tggq4HFqFymyDjTMV/yfv7eGSUkzcX/52ysYFgN	rundll32.exe, 00000005.00000002.461626922.00000000010CA000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.nytimes.com/	msapplication.xml3.14.dr	false		high
http://https://login.microsoftonline.com/common/oauth2/authorize?client_id=9ea1ad79-fdb6-4f9a-8bc3-2b70f96e	{CA463ED7-9599-11EB-90E4-ECF4BB862DED}.dat.14.dr, ~DF018886609A78E0A2.TMP.14.dr	false		high
http://urs-world.com/joomla/nyEGAUlxBMi/vJvW_2B31g3fIm/PJCeDCcMkYuKm3mBUGX2v/CaL9euzPRyB3Opxa/g	loaddll32.exe, 00000001.00000002.463517172.00000000010B0000.00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.463533375.00000000003960000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://urs-world.com/joomla/LeY03GyFH8M9ux9Q/fhlrqhT7AEWHy5S/Gj6LLiVr5gZ24pcdoa/r9hh9gZTx/jUFCXHTg6g	loaddll32.exe, 00000001.00000003.455028914.0000000000A95000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.youtube.com/	msapplication.xml7.14.dr	false		high
http://www.wikipedia.com/	msapplication.xml6.14.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.com/	msapplication.xml.14.dr	false		high
http://www.live.com/	msapplication.xml2.14.dr	false		high
http://urs-world.com/joomlaaL9euzPRyB3Opxa/glJ_2BkxmWXAk4B/fa_2B_2FtCKRxglTM9/4omZ9P4fz/YwGhMR3ktfTd	loaddll32.exe, 00000001.00000003.457824149.0000000000A95000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://under17.com/joomla/bY332Z6nIw/mpCJzusDxBf4026z_/2BrGN0t7fT0r/o1u_2FGT8iB/giLHX9xa5y4nT5/E4muy	{E47F4CBC-9599-11EB-90E4-ECF4BB862DED}.dat.34.dr	false	• Avira URL Cloud: safe	unknown
http://under17.com	rundll32.exe, 00000005.00000002.461626922.00000000010CA000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.reddit.com/	msapplication.xml4.14.dr	false		high
http://www.twitter.com/	msapplication.xml5.14.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.243.114.196	under17.com	Netherlands		31400	ACCELERATED-ITDE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald

Analysis ID:	381725
Start date:	04.04.2021
Start time:	16:00:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	swlsGbeQwT.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.troj.winDLL@15/50@9/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 46.9% (good quality ratio 44.5%) • Quality average: 78.9% • Quality standard deviation: 28.7%
HCA Information:	• Successful, ratio: 80% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 20.50.102.62, 104.43.139.144, 92.122.145.220, 104.43.193.48, 13.88.21.125, 168.61.161.212, 184.30.20.56, 88.221.62.148, 20.190.160.131, 20.190.160.74, 20.190.160.5, 20.190.160.70, 20.190.160.72, 20.190.160.133, 20.190.160.135, 20.190.160.130, 40.126.31.141, 40.126.31.143, 20.190.159.132, 20.190.159.136, 20.190.159.134, 40.126.31.1, 40.126.31.135, 40.126.31.8, 92.122.213.247, 92.122.213.194, 93.184.221.240, 20.54.26.129, 152.199.19.161, 20.82.210.154, 104.215.148.63, 40.76.4.15, 40.112.72.205, 40.113.200.201, 13.77.161.179 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, bing.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, www.tm.a.prd.aadg.trafficmanager.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, go.microsoft.com, login.live.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ie9comview.vo.msecnd.net, wu.ec.azureedge.net, ris-prod.trafficmanager.net, update4.microsoft.com, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, www.tm.a.prd.aadg.akadns.net, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, microsoft.com, skypedataprdcolwus15.cloudapp.net, www.tm.lg.prod.aadmsa.trafficmanager.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/381725/sample/swlsGbeQwT.dll

Simulations

Behavior and APIs

Time	Type	Description
16:01:47	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	document-1048628209.xls	Get hash	malicious	Browse	
	document-1771131239.xls	Get hash	malicious	Browse	
	document-1370071295.xls	Get hash	malicious	Browse	
	document-69564892.xls	Get hash	malicious	Browse	
	document-1320073816.xls	Get hash	malicious	Browse	
	document-184653858.xls	Get hash	malicious	Browse	
	document-1729033050.xls	Get hash	malicious	Browse	
	document-540475316.xls	Get hash	malicious	Browse	
	document-1456634656.xls	Get hash	malicious	Browse	
	document-1376447212.xls	Get hash	malicious	Browse	
	document-1813856412.xls	Get hash	malicious	Browse	
	document-1776123548.xls	Get hash	malicious	Browse	
	document-684762271.xls	Get hash	malicious	Browse	
	document-1590815978.xls	Get hash	malicious	Browse	
	document-66411652.xls	Get hash	malicious	Browse	
	document-415601328.xls	Get hash	malicious	Browse	
	document-69633738.xls	Get hash	malicious	Browse	
	document-779106205.xls	Get hash	malicious	Browse	
	document-2092157215.xls	Get hash	malicious	Browse	
	document-839860086.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
resolver1.opendns.com	document-1048628209.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-69564892.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1813856412.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1776123548.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-647734423.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1579869720.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-895003104.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-806281169.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1747349663.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1822768538.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-583955381.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1312908141.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1612462533.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1669060840.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-921217151.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1641473761.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1570454889.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-116291302.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-110658411.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-584569254.xls	Get hash	malicious	Browse	• 208.67.222.222
urs-world.com	document-1048628209.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1771131239.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-69564892.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1729033050.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1813856412.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1776123548.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-647734423.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1579869720.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-895003104.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-779106205.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-806281169.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-839860086.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1061603179.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-909428158.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1747349663.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1822768538.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1952275091.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-583955381.xls	Get hash	malicious	Browse	• 185.186.244.95

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-719712851.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1312908141.xls	Get hash	malicious	Browse	• 185.186.244.95
under17.com	document-1048628209.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1771131239.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1370071295.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-69564892.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1320073816.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-184653858.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1729033050.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-540475316.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1456634656.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1376447212.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1813856412.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1776123548.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-684762271.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1590815978.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-66411652.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-415601328.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-895003104.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-69633738.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-779106205.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-2092157215.xls	Get hash	malicious	Browse	• 185.243.114.196

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ACCELERATED-ITDE	document-1048628209.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1771131239.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1370071295.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-69564892.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1320073816.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-184653858.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1729033050.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-540475316.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1456634656.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1376447212.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1813856412.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1776123548.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-684762271.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1590815978.xls	Get hash	malicious	Browse	• 185.243.114.196

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-66411652.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-415601328.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-69633738.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-779106205.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-2092157215.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-839860086.xls	Get hash	malicious	Browse	• 185.243.114.196

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{CA463ED5-9599-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7729684322066352
Encrypted:	false
SSDEEP:	96:reZ2Z3p23SCW3SUGSt3SUGGxf3SUGGv2BM3SUGIHxvkO3SvGIHxvYB:reZ2ZZ2LWjtRfuBMdGOm2B
MD5:	9FBA1C07E1729C3EC595E65CE44D96F7
SHA1:	0B34D0ADB06B257B01F751D58213A811114417FF
SHA-256:	A9C64F0AFA8C119B06DD8789B021B5F08A6CA0E8355E5470F754F78B1175765F
SHA-512:	15C1664626D54A63305B93DC9B7F93D12CD9612F29CAD40ED4C6840827AE72C7EF9DE6D5682FBC9451A393407765D794CC4F914173140C1CCE5B9E28939C2F2
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{E47F4CBA-9599-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	50344
Entropy (8bit):	2.0121808454797434
Encrypted:	false
SSDEEP:	96:r2ZRZtS2tCFWtCEGDttCEG1/ftCEG1pFtMtCEGKSpWtCEGKdppXtCEGKdppHy3Jj:r2ZRZw2eWAtyfQtMx7SlMiMw+IUZaRKg
MD5:	AE1CD01437BAA82F8ED66C62B2A0FC98
SHA1:	CD11DD005794DDE73E9F23F7D6ECA41182E264C0
SHA-256:	4DD3D16C6AE713255EAD5A6511DAB322FB2FA6DF0240D1EACF1F6525F9D0F5B2
SHA-512:	129C360B3206D6A6AEF2DA3521CFDBBE4CA4F1F25D907923AA58A326E4550B28C37FB61393EADD394738BEB3D149F4B331B1A4B9036DCE16CACE6AEBA8EE5F25
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{CA463ED7-9599-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{CA463ED7-9599-11EB-90E4-ECF4BB862DED}.dat	
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	43408
Entropy (8bit):	2.51452944352385
Encrypted:	false
SSDEEP:	192:rVZeQK6gkwjJ21WkMg5NbvdYbvpebvFbvzbvGbvcfzKlAfzKlfbvzfzKlZeSOHhw:rbb1tyYMRomifMAfMnfMsrSNr
MD5:	AE94B84A17E078607B13BEE30BA49658
SHA1:	CB3825F6DF789978529A8E4DDD526849BF525827
SHA-256:	BC32E88C3A9292D06EAEC9C14FA315AB8F2742B4080D6AA9E5A4004ADB0C2F00
SHA-512:	EF92F1E43432D39592E76EF27C0A15E023D3273F73B5BD925AD7F45CB6FC2EF401E322D98631EE2F607498260F4AA1BF885C51E7463E3358A5DB5DB0F9F127E5
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E47F4CBC-9599-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27864
Entropy (8bit):	1.8280170576863544
Encrypted:	false
SSDEEP:	96:r0ZrQl6nBSzjJ2eWL0M09SyZ+0gRaRyZ+0gRNZbr:r0ZrQl6nkzjJ2eWL0M09SyZZRyZoZbr
MD5:	28B3D3764AFE6AD27588A108DA4C03F3
SHA1:	E0906BFB36ED13CBA285919BCD16E0498D042981
SHA-256:	D4F4482C98DAC9E3030F7F218C46AECFBF07EBBCABB9A59A29EA202B03CD6D39
SHA-512:	BE8D6D7B257EBDACF391129C867BFAB02DE287D73FD13667ED364BCAD967A114E5EA55C67CFEF8E1AEE14D72B8DCDB1CED05DF8D3FB6E4A9B2ECD72F691 39B7
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E47F4CBE-9599-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27424
Entropy (8bit):	1.8615748348486356
Encrypted:	false
SSDEEP:	96:rqZhQJ6lBSqjS82MWyMyqmAHlTRmAHlsA:rqZhQJ6lkqjR2MWyMyqnR4A
MD5:	CB3BF105FA67BF98C3B16387DD9063A0
SHA1:	2D60AFA0CC347826D63839AA6C4A14B4398E828C
SHA-256:	78C4D248CE088A09C086AE6008F63CF7E344F1C3D0E0AB9A6010D0F244F2360D
SHA-512:	B727081DD879DF1A8CDD79D81BCC207C053534337F4F6C81D7EDC8D8FCD0E10117147FD777453C7EC9974CA6F7C128294306F89437F4E14F1274F8F8B2F3A53
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.095858414557955
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEZDeD94nWimI002EtM3MHdNMNxOEZDeD94nWimI00ObVbkEtMb:2d6NxO+iaSZHKd6NxO+iaSZ76b
MD5:	E3DE08A587F61D1DEA06BCAD61877181

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
SHA1:	D317501E69C7FBAEE0FB7BE3F78779915BBE63E4
SHA-256:	67A0A8BD1F2C2025C11E6E35A10DB966BC04A4B08E559E1AC078E5F7B16F5277
SHA-512:	9D9F4C3A348DC676DB5858BDCC61C320532BE9DAD1DF72161E103D335BF53D969060205FCF17DC9ED96BB7A783560F4628607A2DAB833EC9377720A8DEE85AF
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xa0123909,0x01d729a6</date><accdate>0xa0123909,0x01d729a6</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xa0123909,0x01d729a6</date><accdate>0xa0123909,0x01d729a6</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.111813493703111
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kDQKQ94nWimI002EtM3MHdNMNxe2kDQuc94nWimI00Obkak6EtMb:2d6NxruQKQaSZHKd6NxruQucaSZ7Aa7b
MD5:	55BDF5BFA509771D0C5F002988DD667B
SHA1:	9865119F223DF8625136A07C76AF4E3186D8E4E7
SHA-256:	D2616E3560672FFC1414CF8FB0674AAD64557378589BD5F7F93AF3AF2D19F1E0
SHA-512:	7FEF79CB6A8E9BD82D596C9A06440F4188C5DC2F729F1C50A7385E8343636B91792242C29B46C2B1012BE83A861FA800AA6DFFC558DDE6925F39263755785E07
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xa00b11f1,0x01d729a6</date><accdate>0xa00b11f1,0x01d729a6</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xa00b11f1,0x01d729a6</date><accdate>0xa00d7464,0x01d729a6</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.141068962313454
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLBZVxCZVx94nWimI002EtM3MHdNMNxvLBZVxCZVx94nWimI00ObmZEs:2d6NxvVrxCrxaSZHKd6NxvVrxCrxaSZM
MD5:	DC0E25403939D372E4617520DA54A77B
SHA1:	C4835FD04781EA69623FAFF0C3CE305949B6FB3E
SHA-256:	27D5ACEA9AECC92CCA97DB52A6693800778AFEFB1D761BAD45273C15D3F4AC21
SHA-512:	710FFFCEF60B63FF699AECDB144D3955C797E4F9639FC4AF11CD9E50DA1E1B4D899018038EE02BD5734EC3E6C17DF3D41D532A9D759F866857FAFACC5C7771A
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xa0149b93,0x01d729a6</date><accdate>0xa0149b93,0x01d729a6</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xa0149b93,0x01d729a6</date><accdate>0xa0149b93,0x01d729a6</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.096159758720799
Encrypted:	false
SSDEEP:	12:TMHdNMNxixfaf94nWimI002EtM3MHdNMNxixfaf94nWimI00Obd5EtMb:2d6NxwqaSZHKd6NxwqaSZ7Jjb
MD5:	39C9AED6D2195AE420F2DA2AA4DF5D45
SHA1:	A7ED979023B17534696FB48B6788CD5713BC9B1B
SHA-256:	08CD137A59C4A8CD817EDD5662758194582974830C80D7DC862527164C8B8879
SHA-512:	64759DA41BE86817C1BD967E7E7C66BB1ED87B69EF3973EC97FEC82E70500BE89B064DD7EB1985B32543F030A44CDA3A1589F5C288C7F23CFBD2829FC0B0487
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xa00fd6c9,0x01d729a6</date><acc date>0xa00fd6c9,0x01d729a6</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xa00fd6c9,0x01d729a6</date><accdate>0xa00fd 6c9,0x01d729a6</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.15404278412856
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwBZVxCZVx94nWimI002EtM3MHdNMNxhGwBZVxCZVx94nWimI00Ob8V:2d6NxQCrxCrxaSZHKd6NxQCrxCrxaSZy
MD5:	8A69E600265363A453EFE78EA8FF7691
SHA1:	0BCF5539F523FC6D827A29286BCA2B67EA846B24
SHA-256:	E36F844B18E03070790D1A5F2B3C3C3DD6C9173A2711757E1DE7FA4D7241DB32
SHA-512:	C7120B22AA43CA11AEBF13D2267E1538FF23162AAEE3F697B4C96188CF1D71DEED8F5FA836455CB8DBD7435AF614F9BDE9A893D03894076405C003ED9616206
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xa0149b93,0x01d729a6</date>< accdate>0xa0149b93,0x01d729a6</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xa0149b93,0x01d729a6</date><accdate>0 xa0149b93,0x01d729a6</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.099036194760591
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nZDeD94nWimI002EtM3MHdNMNx0nZDeD94nWimI00ObxEtMb:2d6Nx0BiaSZHKd6Nx0BiaSZ7nb
MD5:	EEC7A63FBFF4318D673535500FAE9308
SHA1:	4AA03B0A60419BC429D770DD6912E471DB9D5269
SHA-256:	C9EF362D2562D1157495BF44C1E31B7A0A02BFA811C75523C447E6573B4A41CA
SHA-512:	B8F77A9BE3E03D69DBF6AA4F6848E8AF2A9393E01B9079C25725BC8D224AE57C8D80A68A7850218009C8B1D9C70BE1042AAD8824BD1A3430D60F581FEBEA31F C
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xa0123909,0x01d729a6</date><a ccdate>0xa0123909,0x01d729a6</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xa0123909,0x01d729a6</date><accdate>0xa 0123909,0x01d729a6</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.1274810756503095
Encrypted:	false
SSDEEP:	12:TMHdNMNxxxfaf94nWimI002EtM3MHdNMNxxxfeD94nWimI00Ob6Kq5EtMb:2d6Nx7qaSZHKd6Nx7iaSZ7ob
MD5:	81670A4B364F26CC25EAA64125904624
SHA1:	886501C8C779388FD276BA39BCF12CC49A1B217A
SHA-256:	6863ECA00BB564B288AA8AD4EDB489724CF2F3458FE4404CDCBAA0CF11F9B244
SHA-512:	B8B9D14E51624330044EFAEF0600A412AF269B93B1409D05814F6FC47A8363C4F7E2CC9CB381BF99A574122D077D4A1478AE2197D45D2A078BCDDCCDA0B2360
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xa00fd6c9,0x01d729a6</date>< accdate>0xa00fd6c9,0x01d729a6</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xa00fd6c9,0x01d729a6</date><accdate>0 xa0123909,0x01d729a6</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.126459394681448
Encrypted:	false
SSDEEP:	12:TMHdNMNxczcuc94nWimI002EtM3MHdNMNxczcaf94nWimI00ObVEtMb:2d6NxScucaSZHKd6NxScqaSZ7Db
MD5:	46209166AB2D08F92A752C6796194255
SHA1:	3F267E7E488C15EB52A8D9C2021092AADD1116DA
SHA-256:	666EB49747BB674C28101455C2C49A9E9DCFF62B7C0C175C0DC24ED6C0CF3836
SHA-512:	DCBAB9AF566056695EB787A8F3801640B9643A3574D4219F368CDD35634DE27A5A0609D4C9FBE688623685CE61CE4F8C40E2EC8F49298BE8DC01C67BDB8E373
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xa00d7464,0x01d729a6</date><accdate>0xa00d7464,0x01d729a6</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xa00d7464,0x01d729a6</date><accdate>0xa00fd6c9,0x01d729a6</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.081960818763466
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnxfaf94nWimI002EtM3MHdNMNxfnxfaf94nWimI00Obe5EtMb:2d6NxVqaSZHKd6NxVqaSZ7ijb
MD5:	58FEF57D9310E7E12BF0110990650EE7
SHA1:	28B55DAD7B7475A40A5A36FFF7F8E040127A6335
SHA-256:	3F67830832DBEB3036E0C46FC928EE2FEF1BEBD80BA3FBB3925FC3E5AD60E3CA
SHA-512:	A6B54DC1AEDF9AFACBCACF9F16BBC740DBEE26D823A4BB350D7A26BF5CDD60AF4C0B0A1ADD0BC12A4356517A2D3AA0F226CE88F5E395F1141EEAD44CAD93A5E0
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xa00fd6c9,0x01d729a6</date><accdate>0xa00fd6c9,0x01d729a6</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xa00fd6c9,0x01d729a6</date><accdate>0xa00fd6c9,0x01d729a6</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\HdepnBaFj-yarvouFUIlfV4Q9D8.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	3201
Entropy (8bit):	5.369958740257869
Encrypted:	false
SSDEEP:	48:rmo6TIPx85uuYPXznTBB0D6e7htJETfD8QJLxDO7KTUx42Z3rtki: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\0W10PBUV\NGDGShwgz5vCvyjNFyZiaPlHGCE.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	252
Entropy (8bit):	4.837090729138339
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\NGDGShwgz5vCvyjNFyZiaPlHGCE.gz[1].js	
SSDEEP:	6:qbLkyK4hImTzBwhLM1whA+XzFE8KSiQLGPQQgnaqza:IQD2IkzaLMGAMzDBVKY+ia
MD5:	1F62E9FDC6CA43F3FC2C4FA56856F368
SHA1:	75ADD74C4E04DB88023404099B9B4AAEA6437AE7
SHA-256:	E1436445696905DF9E8A225930F37015D0EF7160EB9A723BAFC3F9B798365DF6
SHA-512:	6AADAA42E0D86CAD3A44672A57C37ACBA3CB7F85E5104EB68FA44B845C0ED70B3085AA20A504A37DDEDEA7E847F2D53DB18B6455CDA69FB540847CEA6419C DBC
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/NGDGShwgz5vCvyjNFyZiaPlHGCE.gz.js
Preview:	var Button;(function(){WireUp.init("button_init",function(n){var t=n.getAttribute("data-appns"),i=n.getAttribute("data-k");sj_be(n,"click",function(){Log.Log("Click","Button","",!1 ,"AppNS",t,"K",i,"Category","CommonControls")})})})(Button||(Button={}))

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Xp-HPHGHOZznHBwdn7OWdva404Y.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	576
Entropy (8bit):	5.192163014367754
Encrypted:	false
SSDEEP:	12:9mPi891gAseP24yXNbdPd1dPkelrR5MdKIKG/OgrfYc3tOfIvHbt:9mPlP5smDy1dV1dHrLMdKIKG/OgLYgtV
MD5:	F5712E664873FDE8EE9044F693CD2DB7
SHA1:	2A30817F3B99E3BE735F4F85BB66DD5EDF6A89F4
SHA-256:	1562669AD323019CDA49A6CF3BDDECE1672282E7275F9D963031B30EA845FFB2
SHA-512:	CA0EB961E52D37CAA75F0F22012C045876A8B1A69DB583FE3232EA6A7787A85BEABC282F104C9FD236DA9A500BA15FDF7BD83C1639BFD73EF8EB6A910B7529 0D
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/Xp-HPHGHOZznHBwdn7OWdva404Y.gz.js
Preview:	var SsoFrame;(function(n){function t(n){if(n&&n.url&&n.sandbox){var t=sj_ce("iframe"),i=t.style;i.visibility="hidden";i.position="absolute";i.height="0";i.width="0";i.bor der="none";t.src=decodeURIComponent(n.url);t.id="aadssofr";t.setAttribute("sandbox",n.sandbox);_d.body.appendChild(t);n.currentEpoch&&sj_cook.set("SRCHUSR","T", n.currentEpoch,!0,"/");Log&&Log.Log&&Log.Log("ClientInst","NoSignInAttempt","OrgId",!1)}}function i(n){try{n&&n.length===2&&t(n[1])}catch(i){}}n.createFrame=t;n .ssoFrameEntry=i;sj_evt.bind("ssoFrameExists",i,!0,null,!1)})(SsoFrame||(SsoFrame={}))

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\n8-O_KIRNSMPFWQWrGjn0BRH6SM.gz[1].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\0W10PBUV\ozS3T0fsBUPZy4zlY0UX_e0TUwY.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	226
Entropy (8bit):	4.923112772413901
Encrypted:	false
SSDEEP:	6:2LGfGIEW65JcYCgfkF2/WHRMB58IIR/QxbM76Bhl:2RWIyYCwk4/EMB5ZccbM+B/
MD5:	A5363C37B617D36DFD6D25BFB89CA56B
SHA1:	31682AFCE628850B8CB31FAA8E9C4C5EC9EBB957
SHA-256:	8B4D85985E62C264C03C88B31E68DBABDCC9BD42F40032A43800902261FF373F
SHA-512:	E70F996B09E9FA94BA32F83B7AA348DC3A912146F21F9F7A7B5DEEA0F68CF81723AB4FEDF1BA12B46AA4591758339F752A4EBA11539BEB16E0E34AD7EC946763
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/ozS3T0fsBUPZy4zlY0UX_e0TUwY.gz.js
Preview:	(function(n,t,i){if(t){var r=!1,f=function(){r||(r=!0,typeof wlc!="undefined"&&wlc(sj_evt,sj_cook.set,wlc_t))},u=function(){setTimeout(f,t)};n.bind("onP1",function(){i?n.bind("aad:signedout",u):u()},1)}})(sj_evt,wlc_d,wlc_wfa)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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:	E85360DBBB0881792B86DCAF56789434152ED69E00A99202B880F19D551B8C78EEFF38A5836024F5D61DBC36818A39A921957F13FBF592BAAFD06ACB1AED244E
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\MEEXW4H4\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\MEEXW4H4\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:+FE64YTsQF61KWlWeM2lSoiLKiUfplYdk+fzvOMuHMH34tDO8XgGQE3BUf4JPwk:+FdF6UYXEBi9kIHIB1UY
MD5:	EF3DA257078C6DD8C4825032B4375869
SHA1:	35FE0961C2CAF7666A38F2D1DE2B4B5EC75310A1
SHA-256:	D94AC1E4ADA7A269E194A8F8F275C18A5331FE39C2857DCED3830872FFAE7B15
SHA-512:	DBA7D04CDF199E68F04C2FECFDADE32C2E9EC20B4596097285188D96C0E87F40E3875F65F6B1FF5B567DCB7A27C3E9E8288A97EC881E00608E8C6798B24EF3F
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/P3LN8DHh0udC9Pbh8UHnw5FJ8R8.gz.js
Preview:	var Identity=Identity||{},ham_id_js_downloaded=!1;(function(n,t,i,r,u,f,e){e.wlProfile=function(){var r=sj_cook.get,u="WLS",t=r(u,"N"),i=r(u,"C");return i&&e.wlImgSm&&e.wlImgLg?{displayName:t?t.replace(/\+/g," "):"",name:n(t.replace(/\+/g," ")),img:e.wlImgSm.replace(/\{0\}/g,f(i)),imgL:e.wlImgLg.replace(/\{0\}/g,f(i)),idp:"WL"}:null};e.headerLoginMode=0;e.popupAuthenticate=function(n,i,r){var o,u,h,c,v=sb_gt(),l=Math.floor(v/1e3).toString(),s="ct",a=new RegExp("([?&])"+s+"=.*?(&|$)","i");return n.toString()==="WindowsLiveId"&&(o=e.popupLoginUrls,u=o[n],u=u.match(a)?u.replace(a,"$1"+s+"="+l+"$2"):u+"?"+s+"="+l,e.popupLoginUrls.WindowsLiveId=u),(o=e.popupLoginUrls)&&(u=o[n]+(i?"&perms="+f(i):"")+(r?"&src="+f(r):""))&&(h=e.pop(u))&&(c=setInterval(function(){h.closed&&(t.fire("id:popup:close"),clearInterval(c))},100))};e.pop=function(n){return r.open(n,"idl","location=no,menubar=no,resizable=no,scrollbars=yes,status=no,titlebar=no,toolbar=no,width=1000,height=620")};var o=u("id_h"),s=u("id

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\R[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):	373
Entropy (8bit):	7.345815432010222
Encrypted:	false
SSDEEP:	6:XtWRDcqfhdBWQVWf/UOOLlsvRWDhvaSVcM2wMAAlmthHprYkCg+FGZXkrrI1Rx:X8Qqfl/SX4lI8vavMnrYk3BF0cPx
MD5:	8D03D1B04BF7CFDFBD966CE7C7BB8AFA
SHA1:	49EB075B74AA5299891FB5B0FB7728353516F379
SHA-256:	D293C26C80F55B17966EB5799986EEFEC32A3189C3209E0C0233AE33A055309B
SHA-512:	48F747E1FE327BBACA754A8DBEA1DF3B742105FA451C4E9A7121E02D609086BD3C40AAB91B182BFB09EE84E8A01633732062DD9D77EFCE4DF6DC957FCD7C0E0
Malicious:	false
Preview:	.....T.KS.0.....4@.P..F..(..K'..)}..@._.('.;{.%R.C...Ct.3.{...\.DD...\.PE..qC$..5.j.....o.....V..qk..{.-.+.g.\76.....=.'.^..s..=L.DM{.P.....E....n.0....S5...6..O....f.Q.....D..$..1.&.t..=..<[.....'G.....e...(@.X...NA...}J.....W..e...'.,~.M.p8%..K..,.....O.G.>.o..|.D..}.3.v...5..3..u;]..P..y.#E%.p.E@.....K....

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

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\down[1]	
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W..W.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\MEEXW4H4\hsq54HXv3E6bOWi_58PaE6vwTYM.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):	4424
Entropy (8bit):	5.151067247813042
Encrypted:	false
SSDEEP:	96:B3D+ca6IQkQQX6hJmK/Kl9L3vVPTkyfXeJLYLZq76NH:V+ca6IBQQX6aKClFfVPTkyWJLW/
MD5:	FA0E965181E637575B37390656518D0D
SHA1:	06F24D11B54319BE23CDB7C8EEB9D79AAD9CFD06
SHA-256:	4CCC277A590605079234A0C82BFB6C0909B72453D8A45DCACF64463BC429492C
SHA-512:	CA8557ACBC8F7EDEF64FFB0C8A1A7AACE917848FDFA5D3A0ED2867999C6D994DC5E12CEE70E4771C7B0C9C1638071495BD771945FB204B9CFCC589386FFF340
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/hsq54HXv3E6bOWi_58PaE6vwTYM.gz.js
Preview:	define("rmsajax",["require","exports"],function(n,t){function c(){for(var i,n=[],t=0;t<arguments.length;t++)n[t]=arguments[t];if(n.length!=0){if(i=n[n.length-1],n.length==1)ot(i)&&f.push(i);else if(n.length==3){var o=n[0],s=n[1],u=n[2];st(o)&&st(s)&&ot(u)&&(ht(r,o,u),ht(e,s,u))}return window.rms}}function nt(){var i=arguments,n,t;for(o.push(i),n=0;n<i.length;n++)t=i[n],ct(t,r),t.d&&tt.call(null,t);return window.rms}function kt(){var t=arguments,n;for(s.push(t),n=0;n<t.length;n++)ct(t[n],e);return window.rms}function l(){var t,i,n;for(ri(),t=!1,n=0;n<o.length;n++)t=tt.apply(null,p.call(o[n],0))||t;for(i=0;i<s.length;i++)t=ti.apply(null,p.call(s[i],0))||t;if(!t)for(n=0;n<f.length;n++)f[n]()}function tt(){var n=arguments,t,i,f,e;if(n.length===0)return!1;if(t=r[ut(n[0])],n.length>1)for(i=ui.apply(null,n),f=0;f<i.length;f++)e=i[f],e.run=u,dt(e,function(n){return function(){gt(n,i)}}(e));else t.run=u,ft(t,function(){it(t)});return!0}function dt(n,t){var f,u,r;if(!n.state){if(n.state=pt,at(n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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:	dropped
Size (bytes):	327237
Entropy (8bit):	7.97223374454568
Encrypted:	false
SSDEEP:	6144:mBlAVPTvYwTnCCvR2MDIiC0nk6XGvGGHHdsP/5WYAlxI0d1knETax:YAhYwrpY6a8k3OGHHKX5XAlj/Qlx
MD5:	41468B79A1B053BEA7E5139D24020DAC
SHA1:	6E3373EAFE5157DFC4CCEB3B5EDD4A2A8A5D8224
SHA-256:	1736635AF5C198ACC6292C4687385177192D47CD4623495B95A9A81A2DC616D6
SHA-512:	1554B09A56C49BD6D972BDED23D1702E80655898AAE05C77B01D56F0C38A0F783548E78E1AE7CCF96C04201092101DEBC7D2872F59BA921FDE4E744063209938

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\th[1].jpg	
Malicious:	false
Preview:	.....JFIF.....C.....#$&$#.//22//@@@@@@@@@@@@@@@@...C.....%.....%/"...."/*-&&&-*44//44@@>@@@@@@@@@@@@@.. ....8...."..N.....!1."AQa..2q.#BR...br...$3.C...S....%4cs.D..5...&6.T.....7.....!..1AQ."aq..2.B..R...#b..r..3..... ...?.hz.d...V.H...(.....@.....*(..'..@.5...TP.M.54b.3EE....4QV....A...rjrk.....Q..P.M.5.U.9.|.*h..:2h..9.'5.P...FMEM.d.*(.&.....T.P.MFM.P.M.4Q@.4d.E.d...Q@NM..E.d..EE.d ...Q@.4d.Q@NO..4TP..FME....EE.94d..Q@NO..5.P..FM.P..Q.EE.9>u.4T...4d.QR....4P..qQ.E..2h.(.&.&...NM.5.5.2jrj(.$..QE.94d.QB.&..**A95.4Q@.4d.Q@O4d.Q@NM.5 .P..Q..E....FM.P..FO.E....E...Q.SQ..3S.QE.9>td..T...&.(.&..:..@.>u95.P...G5.4..FM...2h...y..(.#&.jj(....(..:....y..(..G54P...h..9.'.(..&...2|.rh.E.sFM..$.>td.Q@.>u95.P.MNME....s.E.. ...E.d.F(...:2|.2h....&.(.&.|...:2j(.'&..(..d..EN(.9...1@G>tsSEE.9..Tb..<..S..T....N(...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\MstqcgNaYngCBavkktAoSE0--po.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	391
Entropy (8bit):	5.184440623275194
Encrypted:	false
SSDEEP:	12:2Qxjl/mLAHPWEaaGRHkj6iLUEkFKgs5qHT:2QC8H+aGRHk+i1kFKgs5qHT
MD5:	55EC2297C0CF262C5FA9332F97C1B77A
SHA1:	92640E3D0A7CBE5D47BC8F0F7CC9362E82489D23
SHA-256:	342C3DD52A8A456F53093671D8D91F7AF5B3299D72D60EDB28E4F506368C6467
SHA-512:	D070B9C415298A0F25234D1D7EAFB8BAE0D709590D3C806FCEAEC6631FDA37DFFCA40F785C86C4655AA075522E804B79A7843C647F1E98D97CCE599336DD9D9
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/MstqcgNaYngCBavkktAoSE0--po.gz.js
Preview:	(function(){function n(){var n=_ge("id_p"),t,i;n&&(t="",i="",n.dataset?(t=n.dataset.src,i=n.dataset.alt):(t=n.getAttribute("data-src"),i=n.getAttribute("data-alt")),t&&t!=""&&(n.onerror=function(){n.onerror=null;n.src="";n.alt=""},n.onload=function(){n.alt=i},n.src=t)}n()})()

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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:vllJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=9002

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\dnserror[1]	
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\eF3rIdIG4fsLyPy7mzgRnjCDKIA[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):	12172
Entropy (8bit):	7.918443542633748
Encrypted:	false
SSDEEP:	192:55tSglBjXtk3RBPvjc6/sB7WYFH+CEWAY7ajZiS8aQoFiJ8VJUsLYpP7:YHHjNsB7WYtFEV1iS8XoFRJbLmP7
MD5:	4CF2646B3478E81FB9444ED499C19310
SHA1:	785DEB21D206E1FB0BC8FCBB9B38119E30832880
SHA-256:	3E3D1F762BE8E3AF89D77E1F291E6228D55FBA619AD6C0763224B4A640D0D9BD
SHA-512:	6CC812012B23313ED2A83706D81B9737C3C6D8EA656FFE8D612006C4C6C03ACCA8428D4C2F89615581F1ACD866925F6DA94F2C66275101558DC8D202E976479
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/eF3rIdIG4fsLyPy7mzgRnjCDKIA.png
Preview:	.PNG.....IHDR...j...t.....PLTE...ttt"""".....""""///...,,,000....}.....*x.%..$..#..$.""",,,....Q".L"~..~.....*:*.....#.....".....---.....O.#.+++.....---.....$.....y..`..G.....).....wwwttt...[[[.....413.....vwzlllqqq.....rxxvxy...vwy.....vwy.....!W.....Y..4f.....uwzwxz.....xxxwxzwwzvvzvwy...vxz.3..0.....l..m..4.....".3.....2..3..l..4.....3..3.....d!.a...?..>..=wxyvwyvwyvv{wxxwxzvxz]ffwwyvwzwwwwzvxzvxywwzwxzvwzwwzwxzwwzvxywwy..>.....!....tRNS..C.....`....C...1.....P.....P.....$`.....@.....j.0.G..p. p.@.`+.``..>^.`..... k@.@.P..p.....0... .....P....``....i...@.. ..0@.....^f....P.

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\4FU4I5GJ.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):	60387
Entropy (8bit):	5.762519122366538
Encrypted:	false
SSDEEP:	1536:GdrSCXrLQ4o3HuzcpUQx3ETOuKsIecFXdAjvd594fJLYvcsbkb097Q53Opw:GhLQt3OwmQxsd59RUew
MD5:	812B06CF552A9865FFC4A460177FE62A
SHA1:	221A73235739FAE5E3155B52E19AB00E2FC37B05
SHA-256:	272F2001B14DD8262789D12B0F906DA5D716D3C08C89DD78D84B1361E685370A
SHA-512:	876748EA811FA6EF35F957E63FA7AD63754874B9EF31D2902D5E28EEDD97C1A6292DDF94C762D6BA0AE0304DC92FF19FEB61B3C7BFCDFB5E46390F88E2C94B4
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.EggTree_ROW9453259256_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=20210404_0700&mkt=de-CH" /><meta property="og:site_name" content="Bing" /><meta property="og:description" content="If you find yourself in Germany or Austria around " /><title>Bing</title><link rel="shortcut icon"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\5rqGloMo94v3vwNVR5OsxDNd8d0[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	461
Entropy (8bit):	4.834490109266682
Encrypted:	false
SSDEEP:	6:tI9mc4sl3WGPXN4x7ZguUz/KVqNFvneuFNH2N9wF+tC77LkeWVLKetCsYuwdOvX0:t41WeXNC1f3q/7H2DIZWYeIsrGYyKYx7
MD5:	4E67D347D439EEB1438AA8C0BF671B6B
SHA1:	E6BA86968328F78BF7BF03554793ACC4335DF1DD
SHA-256:	74DEB89D481050FD76A788660674BEA6C2A06B9272D19BC15F4732571502D94A
SHA-512:	BE40E5C7BB0E9F4C1687FFDDBD1FC16F1D2B19B40AB4865BE81DD5CF5F2D8F469E090219A5814B8DAED3E2CD711D4532E648664BFA601D1FF7BBAA83392D30E
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/5rqGloMo94v3vwNVR5OsxDNd8d0.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 32 32"><title>UserSignedOutIcon</title><circle cx="16" cy="16" r="16" fill="#eee"/><path d="M12.73 13.1a3.271 3.271 0 1 1 3.27 3.2 3.237 3.237 0 0 1-3.27-3.2zm-2.73 9.069h1.088a4.91 4.91 0 0 1 9.818 0h1.094a5.884 5.884 0 0 0-3.738-5.434 4.238 4.238 0 0 0 2.1-3.635 4.366 4.366 0 0 0-8.73 0 4.238 4.238 0 0 0 2.1 3.635 5.878 5.878 0 0 0-3.732 5.434z" fill="#666"/><path fill="none" d="M0 0h32v32h-32z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\6sxhavkE4_SZHA_K4rwWmg67vF0.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	20320

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\6sxhavkE4_SZHA_K4rwWmg67vF0.gz[1].js	
Entropy (8bit):	5.35616705330287
Encrypted:	false
SSDEEP:	384:Kh4xTJXiXZ4sb4ZENXjTDDoFWZ3BnqIfP5IDV6s4RKAvKXAL5Nuwbv++9O:YoTdiJpjBpBnqIH+Z6se4XALueO
MD5:	07F6B49331D0BD13597934A20FAC385B
SHA1:	B39E1439D7FC072AF4961D4AB6DE07D0BC64B986
SHA-256:	4752E030AC235C73E92EC8BBF124D9A32A424457CA9A6D6027A9595DA76F98D7
SHA-512:	333B12B6BC7F72156026829E820A4F24759E15973B474E2FFB264DEE4C50B0E478128255E416F3194E8C170A28DF02AA425D720CC5E15BC2382EA2D6D57A6F5B
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/6sxhavkE4_SZHA_K4rwWmg67vF0.gz.js
Preview:	/*!DisableJavascriptProfiler*/.var BM=BM||{};BM.config={B:{timeout:250,delay:750,maxUrlLength:300,sendlimit:20,maxPayloadSize:14e3},V:{distance:20},N:{maxUrlLength:300},E:{buffer:30,timeout:5e3,maxUrlLength:300},C:{distance:10}},function(n){function vt(){if(!document.querySelector||!document.querySelectorAll){k({FN:"init",S:"QuerySelector"});return}w={};e=[];ft=1;ut=0;rt=0;o=[];s=0;h=!1;var n=Math.floor(Math.random()*1e4).toString(36);t={P:{C:0,N:0,I:n,S:fi,M:r,T:0,K:r,F:0}};vi()}function ei(n,t){var r={};for(var i in n)i.indexOf("_")!==0&&(i in t&&(n[i]!==t[i]||i==="i")?(r[i]=t[i],n[i]=t[i]):r[i]=null);return r}function oi(n){var i={};for(var t in n)n.hasOwnProperty(t)&&(i[t]=n[t]);return i}function b(n,t,r,u){if(!h){k({FN:"snapshot",S:n});return}r=r||gt;t=t||!1;var f=g()+r;ot(o,n)===-1&&o.push(n);t?(yt(),pt(t,u)):f>s&&(yt(),rt=sb_st(pt,r),s=f)}function k(n){var u={T:"CI.BoxModelError",FID:"CI",Name:ht,SV:ct,P:t&&"P"in t?d(t.P):r,TS:f(),ST:v},i,e;for(i in n)u[i]=n[i];e=d(u);wt(e)}func

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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\WJ8I2OL4\bLULVERLX4vU6bjspboNMw9vl_0.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	very short file (no magic)
Category:	downloaded
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A99
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/bLULVERLX4vU6bjspboNMw9vl_0.gz.js
Preview:	0

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\errorPageStrings[1]	
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\WJ8I2OL4\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	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\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):	4.412554678800313
Encrypted:	false
SSDEEP:	3:oVXU17FUTyWIqH8JOGXnE17FUTyWIgn:o9U5FUWWIiqE5FUWWIg
MD5:	11D36C7860FE14809F9264420D47CD90
SHA1:	25F4595DFD3F227E45EA9436D3693159E46E0535
SHA-256:	30F6F4E5353E34087AAB29142A618384BC74DD567096C3FA252B6563709E19E0
SHA-512:	695DF2B7507FA16C76CB53B75B7D783B506974A166D8D8B0D91E861E833580851E666C276B531022A8F3176B0AE73C4BB37885D14F833C9414FF5DFD7A3482F6
Malicious:	false
Preview:	[2021/04/04 16:02:58.148] Latest deploy version: ..[2021/04/04 16:02:58.148] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF018886609A78E0A2.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	53702
Entropy (8bit):	1.4220318854466942
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+6cGPcZpifMAfMnfMhTBofMAfMg:4MSMfMqMSMg
MD5:	EFC22711CC3198F4C920AE3D70B47386
SHA1:	EE38B3E7E5B57498C38A934A4746BD8A48C7136C
SHA-256:	B75DF9ABC6ED9FE716FB0C05CFDFBC2514F2AD0F93D96D50860D3DD695439758
SHA-512:	B5DF8C0EF4DA026E12E6011E411E8ED8BAD2328C65D0BE2B0A9E829FC9B4A9592AF50CD8F824E693F8A7472E39470BACB012675FE22FAC37E06CD0202FDA5E83
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF1781971F6DDEC396.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Temp\~DF1781971F6DDEC396.TMP	
Size (bytes):	39601
Entropy (8bit):	0.5659333175935202
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+/hDqxLyZ+0gRzyZ+0gRXyZ+0gRc:kBqoxKAuqR+/hDqxLyZKyZKyZz
MD5:	F5EC46D360C2DB3589E11DF8EFB77844
SHA1:	1F1F8C5DFCD64E7D0D160D70218D56A12441CF11
SHA-256:	46FDA791A076E9BC1BE427C3809C0920756B4B0774927C7D267BB71FE30AA308
SHA-512:	BC55BC5D0BAB7D9153480C022050E9DA5FFF13D65C46BFBC3B5DCBBEAD1ABE4034DE8FC455DE1316A350E1817638736784631FC07B97FCB6A42F9B904FA46E AA
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFD5883835AA87FACD.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39745
Entropy (8bit):	0.5951299018917467
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+OSDir42mAHlgmAHlomAHl5:kBqoxKAuqR+OIir420Md
MD5:	C31EF9DEBAF503E15BEF41EB128AFF94
SHA1:	63B6B5EA23D114EA7AC0416959A6AEA53FDE625A
SHA-256:	E3B42E0748D0C9286B3D94554EB2735536883D3FB18E89037511FFEB179BBDBF
SHA-512:	DEB658A56778BD5987B1D36569923464587BD4D17563C58C14386F2BD5292193CBC4F591B4ADEA913A4C366C2338E5EFA1D926710112D02187FCE0667FE100F3
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFE3F4BFAB784B55BB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13237
Entropy (8bit):	0.5994303505876222
Encrypted:	false
SSDEEP:	96:kBqoItStMtCEG1pEGKzGKdGFLEGKdGk1GKMLp2:kBqoIMSX
MD5:	42E88EB9215720A98E6693E58AB7059C
SHA1:	B821C69EBB450B7FB4634F7567AAE014C636B728
SHA-256:	48F99F2EE3D823560649FF192F62B6C5DB09DE39EC0CEC24D25A9128C1419EFE
SHA-512:	2F313B1363900085F836DC24C476B1C7DC090750C9EDBE9B8DAE421D33923C597FE831F8EA42A319206B3807631C12364EECB3B0D52402E804A9FF2867D3D1A/
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFEE814DD0E66FBAC9.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.41066654260838553
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo3DF9lo3J9lW3SUGGxZUGIHx2:kBqoI3S3M3SUGGxZUGIHx2
MD5:	9AFCD50C998826ED877B01482E0033EE
SHA1:	B265C9933FE6B3B7454BBE07A0990E60C06E3475
SHA-256:	F99411584A280EE7DCBED4BFD34C883DFFC6559858C069C43D74F205F64C707A
SHA-512:	9D245DE2FEC85809F8E84BB42D5254C2E11DCD8E44992528DA8CF04CBCDA0DCEE259701E9F07D22FC83C456D48DF275D24E75F2282E20DDE43887AC56CD30 EA
Malicious:	false

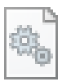
C:\Users\user\AppData\Local\Temp\~DFEE814DD0E66FBAC9.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.561060323428977
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:	swlsGbeQwT.dll
File size:	114200
MD5:	bedfac54b06b97b4de8132d6bfd40de0
SHA1:	e238b2b47e1ccb3ebdadb82eff72125f4747a014
SHA256:	22682ac6f8c484759f44786cc73109993d858a29b25fa15 12196154cf2f0299c
SHA512:	17b3c38e8176a2750d2dcc695a0301848c0b18b8772e8c 20a8a5d3f7c0aed14d4d2d88877493f15d18d4b464babee ff3571b93bf277ce306b8b53650b2258dab
SSDEEP:	1536:DWKaY5Se9WnVI78XvnoxJasJvRHKmyGDvDk0Rt9Y56l5ZMpvV05o9OX5xPw8:DWa0eQnVI7qCqZGDvDk4wol5w0EU
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$......._W...6e..6e..6e..)v..6e...w..6e.Rich.6e.................PE..L.....f`.........!.....Z...........`.......p.....................

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

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

Entrypoint Preview

Instruction
push ebx

Instruction
push ebx
and dword ptr [esp], 00000000h
add dword ptr [esp], ebp
mov ebp, esp
add esp, FFFFFFF8h
push esi
mov dword ptr [esp], FFFF0000h
call 00007FD490BCD580h
push ecx
add dword ptr [esp], 00000247h
sub dword ptr [esp], ecx
push ecx
mov dword ptr [esp], 00005267h
call 00007FD490BC9F29h
push esi
mov esi, eax
or esi, eax
mov eax, esi
pop esi
jne 00007FD490BCF022h
pushad
push 00000000h
mov dword ptr [esp], edi
xor edi, edi
or edi, dword ptr [ebx+0041856Bh]
mov eax, edi
pop edi
push edx
add dword ptr [esp], 40h
sub dword ptr [esp], edx
push ebx
mov dword ptr [esp], 00001000h
push edi
sub dword ptr [esp], edi
xor dword ptr [esp], eax
push 00000000h
call dword ptr [ebx+0045D014h]
mov dword ptr [ebp-04h], ecx
and ecx, 00000000h
xor ecx, eax
and edi, 00000000h
or edi, ecx
mov ecx, dword ptr [ebp-04h]
push eax
sub eax, dword ptr [esp]
or eax, edi
and dword ptr [ebx+0041809Bh], 00000000h
xor dword ptr [ebx+0041809Bh], eax
pop eax
cmp ebx, 00000000h
jbe 00007FD490BCEFFEh
add dword ptr [ebx+004180F7h], ebx
add dword ptr [ebx+00418633h], ebx
mov dword ptr [ebp-04h], edx
sub edx, edx
xor edx, dword ptr [ebx+004180F7h]
mov esi, edx
mov edx, dword ptr [ebp-04h]
push edi
xor edi, dword ptr [esp]
xor edi, dword ptr [ebx+0041856Bh]
and ecx, 00000000h
or ecx, edi
pop edi

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

Data Directories

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

Sections

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

Imports

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

Exports

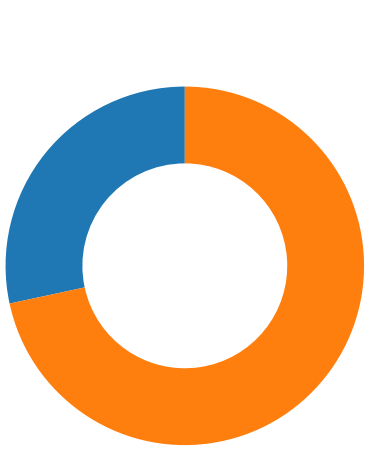
Name	Ordinal	Address
StartService	1	0x1000b959

Network Behavior

Network Port Distribution

Total Packets: 74

- 53 (DNS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 4, 2021 16:02:59.451606989 CEST	49740	80	192.168.2.3	185.243.114.196
Apr 4, 2021 16:02:59.452030897 CEST	49741	80	192.168.2.3	185.243.114.196
Apr 4, 2021 16:03:00.465363026 CEST	49740	80	192.168.2.3	185.243.114.196
Apr 4, 2021 16:03:00.465465069 CEST	49741	80	192.168.2.3	185.243.114.196
Apr 4, 2021 16:03:02.479878902 CEST	49740	80	192.168.2.3	185.243.114.196
Apr 4, 2021 16:03:02.480045080 CEST	49741	80	192.168.2.3	185.243.114.196
Apr 4, 2021 16:03:06.483316898 CEST	49742	80	192.168.2.3	185.243.114.196
Apr 4, 2021 16:03:06.494213104 CEST	49743	80	192.168.2.3	185.243.114.196
Apr 4, 2021 16:03:07.495959044 CEST	49742	80	192.168.2.3	185.243.114.196
Apr 4, 2021 16:03:07.496607065 CEST	49743	80	192.168.2.3	185.243.114.196
Apr 4, 2021 16:03:09.496011972 CEST	49742	80	192.168.2.3	185.243.114.196
Apr 4, 2021 16:03:09.496310949 CEST	49743	80	192.168.2.3	185.243.114.196
Apr 4, 2021 16:03:22.501657009 CEST	49746	80	192.168.2.3	185.243.114.196
Apr 4, 2021 16:03:22.501848936 CEST	49747	80	192.168.2.3	185.243.114.196
Apr 4, 2021 16:03:23.512873888 CEST	49746	80	192.168.2.3	185.243.114.196
Apr 4, 2021 16:03:23.515295029 CEST	49747	80	192.168.2.3	185.243.114.196
Apr 4, 2021 16:03:25.513046026 CEST	49747	80	192.168.2.3	185.243.114.196
Apr 4, 2021 16:03:25.513051987 CEST	49746	80	192.168.2.3	185.243.114.196
Apr 4, 2021 16:03:29.515301943 CEST	49748	80	192.168.2.3	185.243.114.196
Apr 4, 2021 16:03:30.529185057 CEST	49748	80	192.168.2.3	185.243.114.196
Apr 4, 2021 16:03:32.529217005 CEST	49748	80	192.168.2.3	185.243.114.196

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 4, 2021 16:01:29.192274094 CEST	53	56777	8.8.8.8	192.168.2.3
Apr 4, 2021 16:01:29.292031050 CEST	58643	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:01:29.337946892 CEST	53	58643	8.8.8.8	192.168.2.3
Apr 4, 2021 16:01:29.747749090 CEST	60985	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:01:29.793891907 CEST	53	60985	8.8.8.8	192.168.2.3
Apr 4, 2021 16:01:30.666222095 CEST	50200	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:01:30.712429047 CEST	53	50200	8.8.8.8	192.168.2.3
Apr 4, 2021 16:01:31.196697950 CEST	51281	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:01:31.255738974 CEST	53	51281	8.8.8.8	192.168.2.3
Apr 4, 2021 16:01:31.636764050 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:01:31.685570955 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 4, 2021 16:01:32.762422085 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:01:32.808121920 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 4, 2021 16:01:33.871625900 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:01:33.920531034 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 4, 2021 16:01:34.958431959 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:01:35.004554033 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 4, 2021 16:01:36.210057974 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:01:36.255853891 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 4, 2021 16:01:37.136605978 CEST	55984	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 4, 2021 16:01:37.185584068 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 4, 2021 16:01:39.663137913 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:01:39.719099998 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 4, 2021 16:01:40.729192972 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:01:40.775521994 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 4, 2021 16:01:43.202373981 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:01:43.248347044 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 4, 2021 16:01:44.126502037 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:01:44.172966957 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 4, 2021 16:01:45.104238033 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:01:45.152867079 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 4, 2021 16:01:46.448421955 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:01:46.494363070 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 4, 2021 16:01:47.635816097 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:01:47.684720993 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 4, 2021 16:01:50.150437117 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:01:50.199322939 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 4, 2021 16:01:51.571532965 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:01:51.621706963 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 4, 2021 16:01:54.223737001 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:01:54.271368027 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 4, 2021 16:01:55.819143057 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:01:55.870121956 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 4, 2021 16:02:07.001782894 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:02:07.048764944 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 4, 2021 16:02:08.127355099 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:02:08.184216022 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 4, 2021 16:02:14.264333010 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:02:14.323115110 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 4, 2021 16:02:15.604446888 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:02:15.650408983 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 4, 2021 16:02:15.908189058 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:02:15.971019983 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 4, 2021 16:02:16.745093107 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:02:16.810791969 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 4, 2021 16:02:16.833503008 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:02:16.889317989 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 4, 2021 16:02:24.069542885 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:02:24.125868082 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 4, 2021 16:02:24.321078062 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:02:24.377450943 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 4, 2021 16:02:41.267534971 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:02:41.337872982 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 4, 2021 16:02:44.255714893 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:02:44.313371897 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 4, 2021 16:02:45.087198973 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:02:45.143136024 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 4, 2021 16:02:45.260962009 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:02:45.318176031 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 4, 2021 16:02:46.278135061 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:02:46.332463026 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 4, 2021 16:02:48.296119928 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:02:48.342212915 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 4, 2021 16:02:52.307667971 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:02:52.353586912 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 4, 2021 16:02:58.208182096 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:02:58.265595913 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 4, 2021 16:02:59.356476068 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:02:59.427100897 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 4, 2021 16:03:00.917805910 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:03:00.994412899 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 4, 2021 16:03:01.006427050 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:03:01.076920986 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 4, 2021 16:03:01.090979099 CEST	64938	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 4, 2021 16:03:01.148236990 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 4, 2021 16:03:13.504370928 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:03:13.558461905 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 4, 2021 16:03:16.223839998 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:03:16.269764900 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 4, 2021 16:03:18.317326069 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:03:18.372534037 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 4, 2021 16:03:22.195393085 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:03:22.254736900 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 4, 2021 16:03:22.423198938 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:03:22.495955944 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 4, 2021 16:03:34.874150038 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:03:34.940380096 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 4, 2021 16:03:36.207482100 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:03:36.284539938 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 4, 2021 16:03:36.534543037 CEST	63978	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:03:36.588948965 CEST	53	63978	8.8.8.8	192.168.2.3
Apr 4, 2021 16:03:37.541872025 CEST	62938	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:03:37.596290112 CEST	53	62938	8.8.8.8	192.168.2.3
Apr 4, 2021 16:03:48.909156084 CEST	55708	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:03:48.956666946 CEST	53	55708	8.8.8.8	192.168.2.3
Apr 4, 2021 16:03:49.263142109 CEST	56803	53	192.168.2.3	8.8.8.8
Apr 4, 2021 16:03:49.309182882 CEST	53	56803	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 4, 2021 16:02:16.745093107 CEST	192.168.2.3	8.8.8.8	0xcb5d	Standard query (0)	login.microsoftonline.com	A (IP address)	IN (0x0001)
Apr 4, 2021 16:02:59.356476068 CEST	192.168.2.3	8.8.8.8	0xa95d	Standard query (0)	under17.com	A (IP address)	IN (0x0001)
Apr 4, 2021 16:03:13.504370928 CEST	192.168.2.3	8.8.8.8	0x553f	Standard query (0)	under17.com	A (IP address)	IN (0x0001)
Apr 4, 2021 16:03:22.423198938 CEST	192.168.2.3	8.8.8.8	0x9218	Standard query (0)	under17.com	A (IP address)	IN (0x0001)
Apr 4, 2021 16:03:34.874150038 CEST	192.168.2.3	8.8.8.8	0xb6e2	Standard query (0)	urs-world.com	A (IP address)	IN (0x0001)
Apr 4, 2021 16:03:36.207482100 CEST	192.168.2.3	8.8.8.8	0xf877	Standard query (0)	urs-world.com	A (IP address)	IN (0x0001)
Apr 4, 2021 16:03:36.534543037 CEST	192.168.2.3	8.8.8.8	0xcc01	Standard query (0)	under17.com	A (IP address)	IN (0x0001)
Apr 4, 2021 16:03:37.541872025 CEST	192.168.2.3	8.8.8.8	0xbafd	Standard query (0)	urs-world.com	A (IP address)	IN (0x0001)
Apr 4, 2021 16:03:48.909156084 CEST	192.168.2.3	8.8.8.8	0x160c	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 4, 2021 16:02:16.810791969 CEST	8.8.8.8	192.168.2.3	0xcb5d	No error (0)	login.microsoftonline.com	a.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Apr 4, 2021 16:02:16.810791969 CEST	8.8.8.8	192.168.2.3	0xcb5d	No error (0)	a.privatelink.msidentity.com	prda.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Apr 4, 2021 16:02:16.810791969 CEST	8.8.8.8	192.168.2.3	0xcb5d	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 4, 2021 16:02:16.889317989 CEST	8.8.8.8	192.168.2.3	0xa217	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 4, 2021 16:02:59.427100897 CEST	8.8.8.8	192.168.2.3	0xa95d	No error (0)	under17.com		185.243.114.196	A (IP address)	IN (0x0001)
Apr 4, 2021 16:03:13.558461905 CEST	8.8.8.8	192.168.2.3	0x553f	Server failure (2)	under17.com	none	none	A (IP address)	IN (0x0001)
Apr 4, 2021 16:03:22.495955944 CEST	8.8.8.8	192.168.2.3	0x9218	No error (0)	under17.com		185.243.114.196	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 4, 2021 16:03:34.940380096 CEST	8.8.8.8	192.168.2.3	0xb6e2	No error (0)	urs-world.com		185.186.244.95	A (IP address)	IN (0x0001)
Apr 4, 2021 16:03:36.284539938 CEST	8.8.8.8	192.168.2.3	0xf877	No error (0)	urs-world.com		185.186.244.95	A (IP address)	IN (0x0001)
Apr 4, 2021 16:03:36.588948965 CEST	8.8.8.8	192.168.2.3	0xcc01	No error (0)	under17.com		185.243.114.196	A (IP address)	IN (0x0001)
Apr 4, 2021 16:03:37.596290112 CEST	8.8.8.8	192.168.2.3	0xbafd	No error (0)	urs-world.com		185.186.244.95	A (IP address)	IN (0x0001)
Apr 4, 2021 16:03:48.956666946 CEST	8.8.8.8	192.168.2.3	0x160c	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6104 Parent PID: 5828

General

Start time:	16:01:35
Start date:	04/04/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\swlsGbeQwT.dll'
Imagebase:	0x130000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.283968924.0000000003138000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.283941629.0000000003138000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.283743972.0000000003138000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.283981792.0000000003138000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000001.00000002.462142613.00000000009C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.283911802.0000000003138000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.283659543.0000000003138000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.283820403.0000000003138000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.327016038.0000000002FBB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.406489118.0000000002EBD000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.283873534.0000000003138000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	low

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: 4832 Parent PID: 6104

General

Start time:	16:01:35
Start date:	04/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\swlsGbeQwT.dll',#1
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 5076 Parent PID: 6104

General

Start time:	16:01:36

Start date:	04/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\swlsGbeQwT.dll,StartService
Imagebase:	0x11d0000
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: 00000004.00000002.228615251.0000000001180000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 3512 Parent PID: 4832

General

Start time:	16:01:36
Start date:	04/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\swlsGbeQwT.dll',#1
Imagebase:	0x11d0000
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: 00000005.00000003.332207803.0000000005AE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.332108826.0000000005AE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.332246641.0000000005AE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.332181859.0000000005AE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000005.00000002.463340848.0000000003570000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.332262549.0000000005AE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.332227355.0000000005AE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.332279933.0000000005AE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.332152085.0000000005AE8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6320 Parent PID: 792

General

Start time:	16:02:12
Start date:	04/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6f22e0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 6392 Parent PID: 6320

General

Start time:	16:02:13
Start date:	04/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6320 CREDAT:17410 /prefetch:2
Imagebase:	0xd0000
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: 5316 Parent PID: 792

General

Start time:	16:02:56
Start date:	04/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6f22e0000
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: 5340 Parent PID: 5316

General

Start time:	16:02:57
Start date:	04/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5316 CREDAT:17410 /prefetch:2
Imagebase:	0x10c0000
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: 5736 Parent PID: 5316

General

Start time:	16:02:59
Start date:	04/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5316 CREDAT:17416 /prefetch:2
Imagebase:	0x10c0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis