ID: 324124
Sample Name: 2tsY1gtYQe.exe
Cookbook: default.jbs
Time: 12:01:04
Date: 28/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

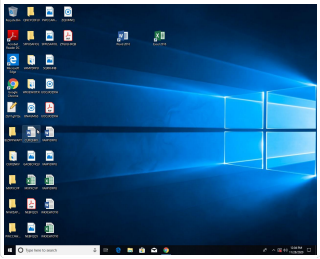
Analysis Report 2tsY1gtYQe.exe

Overview

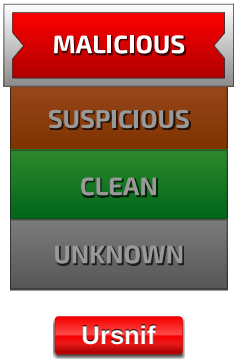
General Information

Sample Name:	2tsY1gtYQe.exe
Analysis ID:	324124
MD5:	75dd85a6d1389e..
SHA1:	39d33f5c7aa2364.
SHA256:	2b120acc21bb14..
Tags:	exe Gozi ISFB Ursnif

Most interesting Screenshot:



Detection

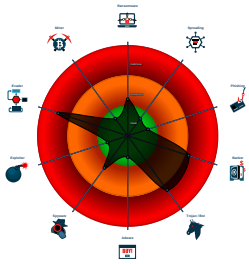


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Creates a COM Internet Explorer ob…
- 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 check if a d…

Classification



Startup

- **System is w10x64**
- 2tsY1gtYQe.exe (PID: 6536 cmdline: 'C:\Users\user\Desktop\2tsY1gtYQe.exe' MD5: 75DD85A6D1389E53FB125EBD9D2711A3)
- iexplore.exe (PID: 6580 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 768 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6580 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 5532 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5504 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5532 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 6824 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6312 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6824 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "server": "12",
  "version": "250162",
  "uptime": "353hh|",
  "crc": "1",
  "id": "1001",
  "user": "4229768108f8d2d8cdc8873a7f098255",
  "soft": "3"
}
```


Yara Overview

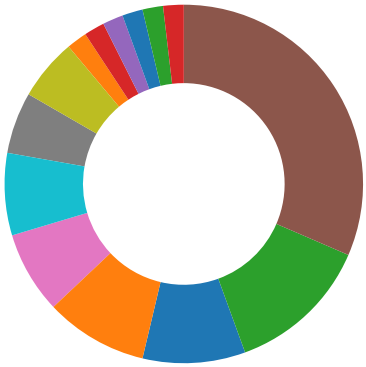
Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.713969974.0000000003248000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.810687783.0000000002FCD000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.810749079.0000000002FCD000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.810673766.0000000002FCD000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.713981277.0000000003248000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 9 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

Creates a COM Internet Explorer object

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Writes or reads registry keys via WMI

Writes registry values via WMI

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

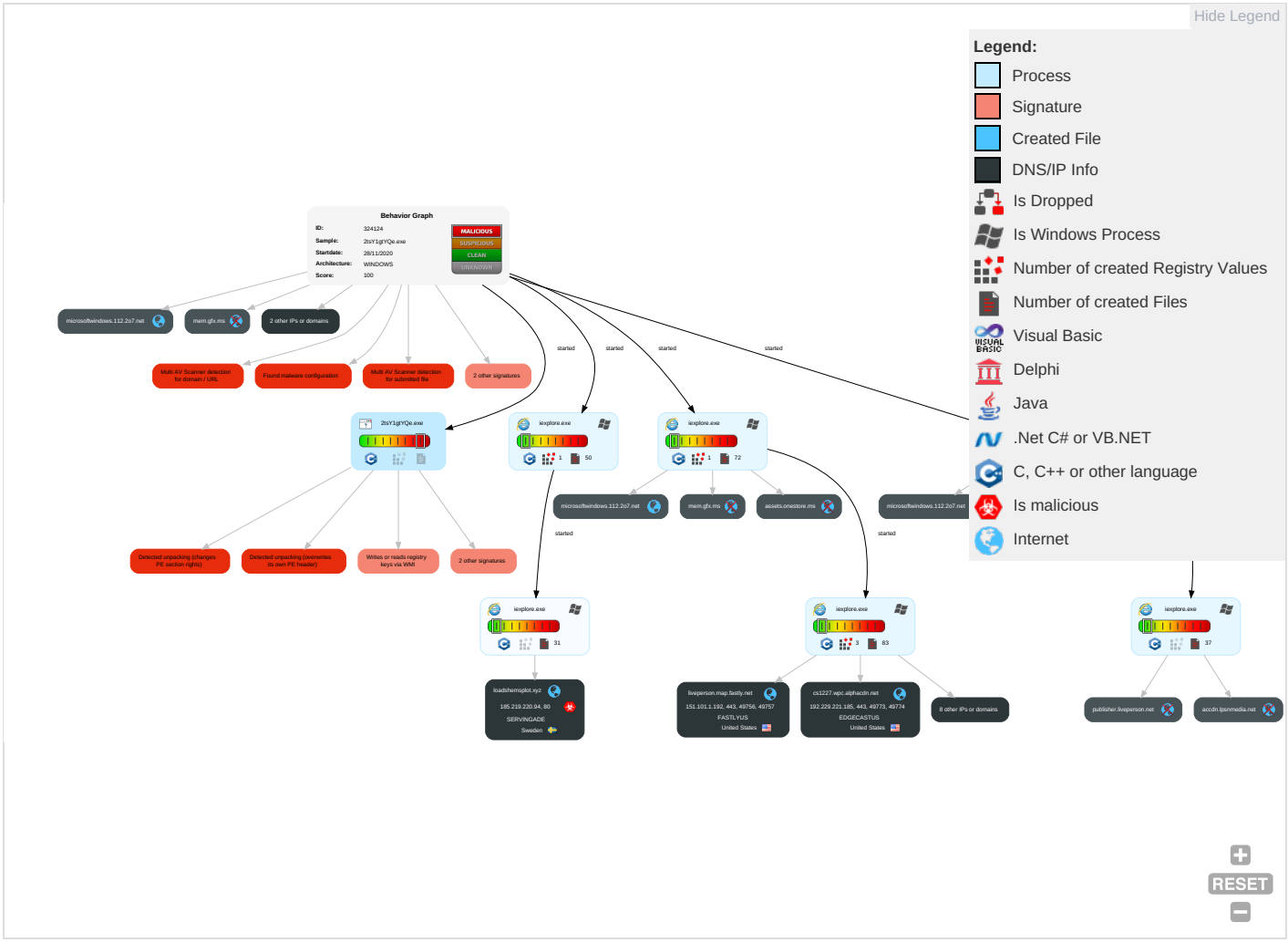
Remote Access Functionality:

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
Valid Accounts	Windows Management Instrumentation 2	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop Insecure Network Communic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS Redirect P Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 2	Security Account Manager	Security Software Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Virtualization/Sandbox Evasion 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 2 3	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Account Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Owner/User Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Access Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	File and Directory Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 2 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cel Base Stati

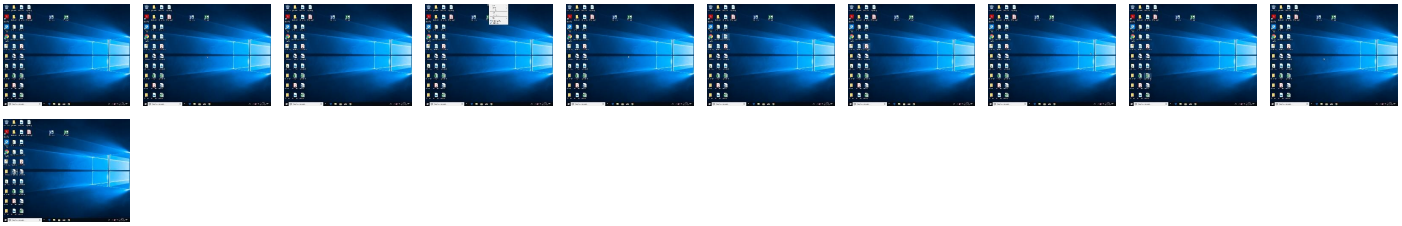
Behavior Graph



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
2tsY1gtYQe.exe	63%	Virustotal		Browse
2tsY1gtYQe.exe	83%	ReversingLabs	Win32.Trojan.Ranumbot	
2tsY1gtYQe.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.2tsY1gtYQe.exe.2540000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
1.2.2tsY1gtYQe.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
1.3.2tsY1gtYQe.exe.a50000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
loadshemsplot.xyz	6%	Virustotal		Browse
cs1227.wpc.alphacdn.net	0%	Virustotal		Browse
liveperson.map.fastly.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://assets.onestore.ms	0%	URL Reputation	safe	
http://https://assets.onestore.ms	0%	URL Reputation	safe	
http://https://assets.onestore.ms	0%	URL Reputation	safe	
http://https://www.microsoftstore.com.cn/hardware/accessories/xbox	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/meversion?partner=MSHomePage&market=de-ch&uhf=1	0%	URL Reputation	safe	
http://https://mem.gfx.ms/meversion?partner=MSHomePage&market=de-ch&uhf=1	0%	URL Reputation	safe	
http://https://mem.gfx.ms/meversion?partner=MSHomePage&market=de-ch&uhf=1	0%	URL Reputation	safe	
http://https://www.microsoftstore.com.cn/xbox	0%	Avira URL Cloud	safe	
http://https://www.21vbluecloud.com/dynamics365/	0%	Avira URL Cloud	safe	
http://https://www.microsoftstore.com.cn/hardware/surface	0%	Avira URL Cloud	safe	
http://https://www.microsoftstore.com.cn/checkout	0%	Avira URL Cloud	safe	
http://https://www.microsoftstore.com.cn/cart	0%	Avira URL Cloud	safe	
http://https://www.microsoftstore.com.cn/hardware/xbox	0%	Avira URL Cloud	safe	
http://https://www.microsoftstore.com.cn/surface	0%	Avira URL Cloud	safe	
http://https://www.microsoftstore.com.cn/software/microsoft-365	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms	0%	URL Reputation	safe	
http://https://mem.gfx.ms	0%	URL Reputation	safe	
http://https://mem.gfx.ms	0%	URL Reputation	safe	
http://https://release.moscnuat.com	0%	Avira URL Cloud	safe	
http://https://www.microsoftstore.com.cn/hardware/accessories/surface	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://https://www.microsoftstore.com.cn/microsoft-365/microsoft-365	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
microsoftwindows.112.2o7.net	15.237.136.106	true	false		high
dh1y47vf5ttia.cloudfront.net	143.204.215.116	true	false		high
loadshemsplot.xyz	185.219.220.94	true	true	• 6%, Virustotal, Browse	unknown
cs1227.wpc.alphacdn.net	192.229.221.185	true	false	• 0%, Virustotal, Browse	unknown
liveperson.map.fastly.net	151.101.1.192	true	false	• 0%, Virustotal, Browse	unknown
logincdn.msauth.net	unknown	unknown	false		unknown
accdn.lpsnmedia.net	unknown	unknown	false		high
publisher.liveperson.net	unknown	unknown	false		high
assets.onestore.ms	unknown	unknown	false		unknown
lptag.liveperson.net	unknown	unknown	false		high
static-assets.fs.liveperson.com	unknown	unknown	false		high
mem.gfx.ms	unknown	unknown	false		unknown

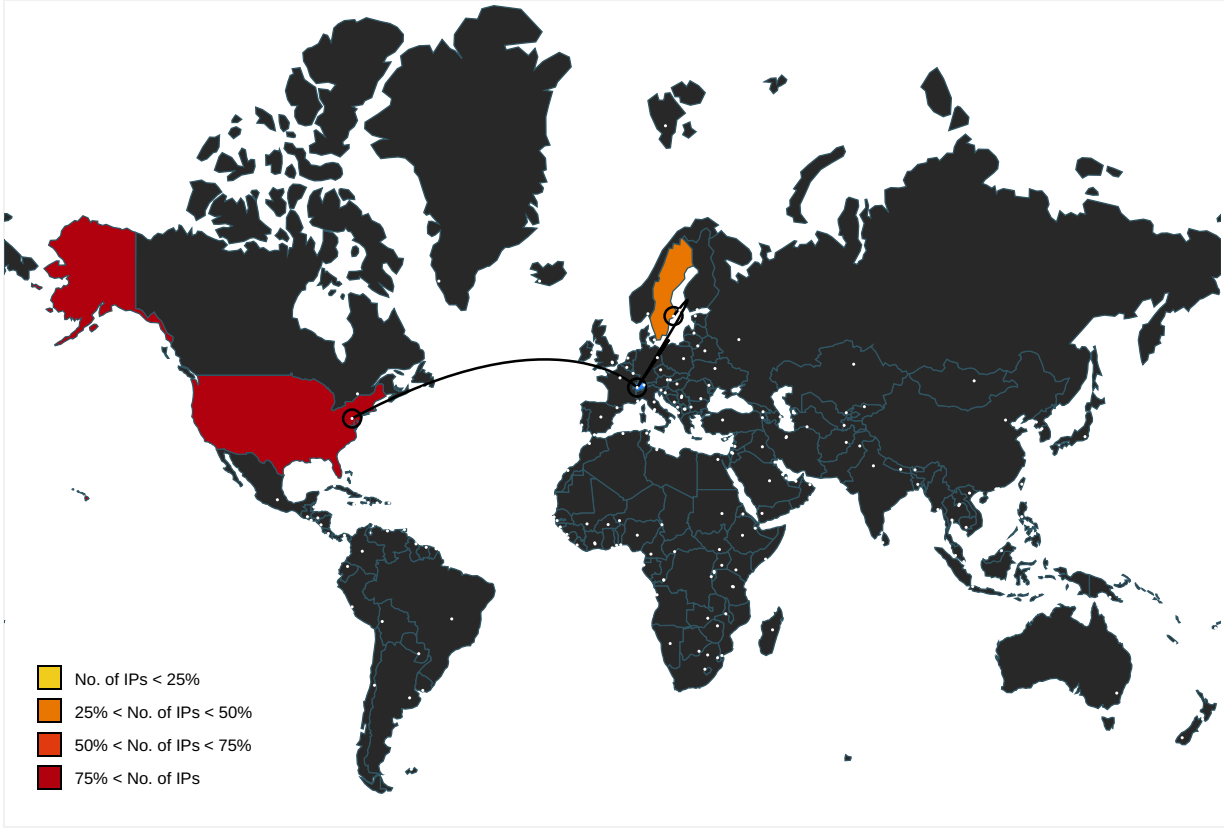
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.live.com/owa/	de-ch[1].htm.15.dr	false		high
http://https://support.office.com/de-de/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://www.onenote.com/?omkt=de-CH	de-ch[1].htm.15.dr	false		high
http://https://support.office.com/es-co/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://products.office.com/de-ch/academic/compare-office-365-education-plans	de-ch[1].htm.15.dr	false		high
http://https://assets.onestore.ms	de-ch[1].htm.15.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://support.office.com/tr-tr/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://www.skype.com/de/	de-ch[1].htm.15.dr	false		high
http://www.amazon.com/	msapplication.xml.4.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://static-assets.fs.liveperson.com/microsoft/lp_ada_enhancements-prod.css	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://www.microsoftstore.com.cn/hardware/accessories/xbox	iframe[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://www.twitter.com/	msapplication.xml5.4.dr	false		high
http://https://publisher.liveperson.net/iframe-le-tag/iframe.html?lpsite=60270350&lpsection=store-sales	de-ch[1].htm.15.dr	false		high
http://https://support.office.com/zh-tw/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://support.office.com/zh-hk/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://support.office.com/en-ca/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://support.office.com/pt-pt/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://mem.gfx.ms/meversion?partner=MSHomePage&market=de-ch&uhf=1	de-ch[1].htm.15.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://support.office.com/sk-sk/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://support.office.com/ja-jp/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://va.idp.liveperson.net	iframe[1].htm.5.dr	false		high
http://https://support.office.com/ar-sa/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://www.microsoftstore.com.cn/xbox	iframe[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.instagram.com/microsoftch/	de-ch[1].htm.15.dr	false		high
http://https://support.office.com/sv-se/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://support.office.com/vi-vn/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://support.office.com/es-es/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://www.21vbluecloud.com/dynamics365/	lp_ada_enhancements-prod[1].js.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.microsoftstore.com.cn/hardware/surface	iframe[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://support.office.com/en-gb/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://support.office.com/ko-kr/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://support.office.com/nb-no/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://support.office.com/pt-br/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://publisher.liveperson.net	de-ch[1].htm.15.dr	false		high
http://https://support.office.com/hu-hu/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://support.office.com/da-dk/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://www.reddit.com/	msapplication.xml4.4.dr	false		high
http://https://support.office.com/de-ch/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://www.microsoftstore.com.cn/checkout	iframe[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	social[1].js.5.dr	false		high
http://www.nytimes.com/	msapplication.xml3.4.dr	false		high
http://https://developer.mozilla.org/en-US/docs/Web/Accessibility/ARIA/Roles/Alert_Role	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://support.office.com/en-in/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://microsoftwindows.112.2o7.net	de-ch[1].htm.15.dr	false		high
http://https://onedrive.live.com/about/de-ch/	de-ch[1].htm.15.dr	false		high
http://https://support.office.com/en-ie/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://github.com/requirejs/requirejs/LICENSE	de-ch[1].htm.15.dr	false		high
http://https://lpcdn.lpsnmedia.net	iframe[1].htm.5.dr	false		high
http://https://support.office.com/en-ae/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://va.msg.liveperson.net	iframe[1].htm.5.dr	false		high
http://https://www.microsoftstore.com.cn/cart	iframe[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.microsoftstore.com.cn/hardware/xbox	iframe[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://support.office.com/zh-cn/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.microsoftstore.com.cn/surface	iframe[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://support.office.com/es-mx/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://support.office.com/th-th/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://www.youtube.com/user/MicrosoftCH	de-ch[1].htm.15.dr	false		high
http://https://support.office.com/nl-nl/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://www.microsoftstore.com.cn/software/microsoft-365	iframe[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://support.office.com/en-us/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://mem.gfx.ms	de-ch[1].htm.15.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://support.office.com/id-id/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://release.moscnuat.com	iframe[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://github.com/requirejs/domReady	de-ch[1].htm.15.dr	false		high
http://https://support.office.com/fi-fi/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://schema.org/ItemList	de-ch[1].htm.15.dr	false		high
http://https://lpcdn.lpsnmedia.net/le_unified_window/9.12.0.19-release_4769/resources/loader_on_warmGray5_7	iframe[1].htm.5.dr	false		high
http://https://support.office.com/fr-ch/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://twitter.com/microsoft_ch	de-ch[1].htm.15.dr	false		high
http://https://support.office.com/es-cl/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://support.office.com/he-il/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://support.office.com/en-za/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://support.office.com/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://support.office.com/pl-pl/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://support.office.com/ru-ru/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://www.youtube.com/	msapplication.xml7.4.dr	false		high
http://https://support.office.com/fr-fr/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://www.linkedin.com/company/1035	de-ch[1].htm.15.dr	false		high
http://https://www.microsoftstore.com.cn/hardware/accessories/surface	iframe[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown
http://www.wikipedia.com/	msapplication.xml6.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://support.office.com/cs-cz/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://support.office.com/en-ng/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://support.office.com/it-it/article/get-support-or-advice-18948a4c-3eb1-4b30-b1bc-a4cc29eb7655	lp_ada_enhancements-prod[1].js.5.dr	false		high
http://https://www.xbox.com/	de-ch[1].htm.15.dr	false		high
http://github.com/aFarkas/lazysizes	de-ch[1].htm.15.dr	false		high
http://www.live.com/	msapplication.xml2.4.dr	false		high
http://schema.org/Organization	de-ch[1].htm.15.dr	false		high
http://https://channel9.msdn.com/	de-ch[1].htm.15.dr	false		high
http://https://www.microsoftstore.com.cn/microsoft-365/microsoft-365	iframe[1].htm.5.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
151.101.1.192	unknown	United States		54113	FASTLYUS	false
192.229.221.185	unknown	United States		15133	EDGECASTUS	false
185.219.220.94	unknown	Sweden		39378	SERVINGADE	true
143.204.215.116	unknown	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324124
Start date:	28.11.2020
Start time:	12:01:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2tsY1gtYQe.exe
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:	23
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:	mal100.bank.troj.evad.winEXE@10/83@20/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 32.5% (good quality ratio 31.5%) • Quality average: 81.7% • Quality standard deviation: 26.3%
HCA Information:	• Successful, ratio: 73% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.147.198.201, 104.42.151.234, 104.83.120.32, 40.112.72.205, 104.215.148.63, 13.77.161.179, 40.76.4.15, 40.113.200.201, 92.122.145.53, 104.83.98.153, 13.107.246.13, 104.83.97.40, 92.122.213.247, 92.122.213.194, 65.55.44.109, 152.199.19.160, 178.249.101.23, 23.210.249.93, 178.249.97.99, 40.90.137.127, 40.90.137.124, 40.90.23.153, 40.90.23.247, 40.90.23.208, 40.90.137.120, 40.90.23.154, 13.104.215.69, 51.104.139.180, 40.88.32.150, 52.155.217.156, 2.20.142.210, 2.20.142.209, 20.54.26.129, 152.199.19.161, 40.90.23.68, 40.90.22.186, 40.90.22.185, 40.90.22.190, 40.90.22.188, 40.90.22.184, 40.90.22.191, 40.90.22.183, 23.211.5.92, 40.90.22.192, 40.90.23.63, 40.90.22.187, 40.90.22.189 • Excluded domains from analysis (whitelisted): assets.onestore.ms.edgekey.net, arc.msn.com.nsatc.net, publisher.livepersonk.akadns.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, www.microsoft.com-c-3.edgekey.net, shop.microsoft.com, star-azurefd-prod.trafficmanager.net, login.live.com, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, e10583.dspg.akamaiedge.net, global.vortex.data.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, lgincdnvzeuno.ec.azureedge.net, assets.onestore.ms.akadns.net, web.vortex.data.trafficmanager.net, c-s.cms.ms.akadns.net, ris.api.iris.microsoft.com, t-0003.t-msedge.net, e55.dspb.akamaiedge.net, lgincdn.trafficmanager.net, cdn.account.microsoft.com.akadns.net, blobcollector.events.data.trafficmanager.net, c.s-microsoft.com-c.edgekey.net, www.tm.lg.prod.aadmsa.trafficmanager.net, cs9.wpc.v0cdn.net, au.download.windowsupdate.com.edgesuite.net, a1449.dscg2.akamai.net, arc.msn.com, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, iecvlist.microsoft.com, go.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, bay-main-ips-v4only.b.lg.prod.aadmsa.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, cs22.wpc.v0cdn.net, ie9comview.vo.msecnd.net, mem.gfx.ms.edgekey.net, accdn.lpsnmedia.livepersonk.akadns.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, login.msa.msidentity.com, web.vortex.data.microsoft.com, lptag.liveperson.cotcdb.net.livepersonk.akadns.net, lgincdnvzeuno.azureedge.net, skypedataprdcoleus16.cloudapp.net, c.s-microsoft.com, go.microsoft.com.edgekey.net, e13678.dscg.akamaiedge.net, az725175.vo.msecnd.net, skypedataprdcolwus16.cloudapp.net, www.microsoft.com, e13678.dspb.akamaiedge.net, wcpstatic.microsoft.com • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.229.221.185	http://https://34.75.2o2.lol/XYWNc0aW9uPWwNsaWNrJngVybD1ovndHRwnczovL3NleY3wVyZWQtbG9naW4ubmV0nL3BhZ2VzLzQyY2FkNTJhZmU3YSZyZWNpcGllbnRfaWQ9NzM2OTg3ODg4JmNhbXBhaWduX3J1bl9pZD0zOTM3OTcz	Get hash	malicious	Browse	
	PAYMENT RECEIPT.html	Get hash	malicious	Browse	
	http://searchlf.com	Get hash	malicious	Browse	
	http://https://pembina.sharepoint.com/teams/BOandP/_layouts/15/guestaccess.aspx?share=Ev8UHcgPkQRPnPpDIa8PTeUBDnUZj2epg0IcLzD6O0XQNQ&e=5:GyiSQ3&at=9	Get hash	malicious	Browse	
	http://218.44.255.241/wp-includes/js/nri.exe	Get hash	malicious	Browse	
	http://https://flyboyfurnishings.com/firstam/RD-FITT	Get hash	malicious	Browse	
	http://https://aterapeutica.com.br/link	Get hash	malicious	Browse	
	http://https://honcdestruction-shared.com/ViewHonc-SharedInfo	Get hash	malicious	Browse	
	Payment Receipt.html	Get hash	malicious	Browse	
	REMITTANCE _REPORT 00189_docx.html	Get hash	malicious	Browse	
	REMITTANCE _REPORT 00189_docx.html	Get hash	malicious	Browse	
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fmib14.mailinblack.com%2fsecurelink%2f%3fkey%3deyJ1cmwiOiJodHRwczovL2xpbmtwcm90ZWN0LmN1ZGFzdmMuY29tL3VybD9hPWh0dHBzJTNhJTJmJTJmbWliMTQubWFpbGluYmxhY2suY29tJTJmc2VjdXJlbGluayUyZiUzZmtleSUzZGV5SjFjbXdpT2lKb2RIUndjem92TDI5dGJtbHdhR0Z5YlMxdGVTNXphR0Z5WlhCdmFXNTBMbU52YlRvME5ETXZPbUk2TDJjdmNHVnljMjl1WVd3dlpHbHlaV04wYVc5dVgzRjFZV3hwZEdWZmIyMXVhWEJvWVhKdFgyWnlMMFZtU1ZJM1lYTllOV2hvVDJjeGJsaDJSek5MYTBOQlFrTmpkemM0WTBKRFJWVlFUVGh1YTNoM2FYRkhOR2MlMmZaVDAwSlROaGNtRTRWa2xDSm1GMFBUa2lMQ0pzWVc1bklqb2lSbElpTENKMGIydGxiaUk2SW1kQlFVRkJRVUptY25CWWVWZG5TMlJVVTIxcFFYWnhhRTExTVhCTVNVeDJWVXB5TmxOV1FVMVdkVFJDTkVWc1RtdEdkV0UyYW1GNE1VNUNZVkZEVGtreWVHUk1hbVZoYTJaWWVqTmFlWHBHT0VkT1JuQjJiM2xrV0hSSFNqRnJiWFpQYjBSbVZtbHVSemRUVFhGQ00xSnhXbUpqYVdSelIzSjZkV0ZXTUZOWVdISnVVa3BtWW5CcFNXYzRiMEpPWkdWVk9lRnZTSGhqVkVkelQyOWtMVnBwWDNKZmEwaGZPR1pJZEZGbVMwaDRaWFJ4TW5reGNucDBhelZDWWpKemEycE9WREV5Y1dSdmJUQTJXVmhTUTBSMlpHTkROVU5vVjBKd2JHUkpaMWw1WDJRMlQzQjZUMk5SWDJ4a05YUTBOSFl5VFhsZlNlWjVTalZRU0hWbVRtbEdSa1ZvY0ZORFVXSnphalZEYkdZMldFeHlibUp2Y0ZSaWMwUnFiRk10WWtrelh6TnNTbE5UWWtWWlIVMUtUWE5MU0U1RGJHeEpTRlJPVUZOTU9FVnJVM3B6WldaT2QxWldURGxRSW4wJTNkJmM9RSwxLHVPS0RmZDhQNXpDV0dpSjduYWJRZTF0TUtJLXQ1RWVRRDVhTUNhRkgwWm5RTkptbF9FTldFQ3RjMGh5VmpndHVxVjlGWnN2aGlaRjNJYWR4T29oZ0RFYm9XUVpYaFB3Y2JXaXVWaGt1UDBNcEFXeUwwU3hWYXBmVXlsbGEmdHlwbz0xIiwibGFuZyI6IkZSIiwidG9rZW4iOiJnQUFBQUFCZnJwaGYxRXp0eTRiT3ZUbHVMTG82X2IyNk80ZFljaTJTU0htYzJ0QVNSbUpjbVVheHNLNTNEUXdoenVJelRXZkdrRGxFR1RCYkQtWjJYOVlyOWZobUR5R0FSQS1GNURrcE5ad0tKeDZtWlRRcHZGbUxhZy1saTluTS0zMWtkX2lOU09iTXY1eXZfX2JhNGVaa05UVm4yUHR5cUZZQXZWeFhQT2ViU2t4T3RUT0lzbVJ5OUZMQmhEQUl0bFh6bEJydzVDbTY4MjVnV0p0LUtmT2lrX0IxYTV6aE5fX0RTNGZEZWJFb3dKcDlhYkZFQXR3ZG00dFVud0hnTXVCcWFmUkRrWVBvUjUwQlRXSFZRRE0zY0UxbzhhRWxWTk81bjRNVjhGOC1VbGdTRlN6TTFpaFB1eF95bDQ2Q2FlMDFGREh1RmVPWiJ9&c=E,1,1tkd_Vao5V7MBpjt2HGhT95VYqfomvyWqF9-x-vgjffraTPXpntiypw4qSf4ZB8PffL3lyrHkViyszaFbvr2EYVjik6RcG-ITO1uye5rd9JQCgk,&typo=1	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://view.microsoftstoreemail.com/?qs=919b7aef4d37fc9759bdc61c9ec1eab8ab462245013a6c5570660677da5b9c71b0398c590628a4a81fcf100f878508057da976e103d9620c83e65f4ff4c5fed6e41efb0579ab41cb77f4a2a59f041aca3c6ee4336b7444aa	Get hash	malicious	Browse	
	MicrosoftEmail-Reactivation.html	Get hash	malicious	Browse	
	http://https://40.90.22.191/	Get hash	malicious	Browse	
	http://https://warrantgroupsrl.sharepoint.com/:f:/s/Accounts/EhCnAgtYLUREispUzaCeN1oB9Po_DSj3QGTNlHNAcUQjqQ?e=5%3aSV525M&at=9	Get hash	malicious	Browse	
	Remittance.html	Get hash	malicious	Browse	
	http://https://docsharex-authorize.firebaseapp.com/common/oauth2/authorize-client_id-43435a7b9-9a363-49130-a426-35363201d503&redirect_uri-www-office-com-response_type-code-id_token&scope-openid-profile&response_mode-form_post&nonce-637402967941920791-Y2FkNjEzMmQtZTE1NC00NjBkLWFiOTYtOWExMDcwYTJlM2Q2N2ZlMDIwNjctOWIyYS00MzZhLWI0NjctYzI3NmM2OGIxZmE4&ui_locales=en-US&mkt=en-US&client-request-idaa28d8e1-058b-4002-a687-8a271de76ed6&state=7ynxU_43bB49ObxK6fyeLMFrS5Zpa0bLtGntUmD69Tf91ft_9m0BSx-GAdmxHr-754MYwJ7SDAghFNzHZnzawCzy-zaIEk46cGCcIr6GURMILdMGTns7hrsMTD9is8TceX7Qd5lzrcNVEq5hVApCi7o5WfvLBB23SkrUp7UjYnPdzaL8RXV-H9Vd_qceEdXDC7ZV6qACMIlYZgfChx1sAsnIT35gVD1UVbrkTDRpTSx8a66JQlYsfUO03GJhGgaeyflaCA-WXTIn2Fb3QljMHQ&x	Get hash	malicious	Browse	
	http://https://nam02.safelinks.protection.outlook.com/ap/b-59584e83/?url=https%3A%2F%2Fnetorg537767-my.sharepoint.com%2F%3Ab%3A%2Fg%2Fpersonal%2Fross_normanrubininc_com%2FEYkCOGLj2o5Lrb-ttgE9hQ4BcIWbpU-30zTSNy9QGLnLQg%3Fe%3D4%253aZSw9hJ%26at%3D9&data=04%7C01%7Cmaria.collito%40benefitmall.com%7C4c4a56b70fb64f2f8f0a08d88377a939%7Cd5254c64bea1491da6a09719464ce9db%7C0%7C0%7C637403899190134786%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0&sdata=iT1UxB9gxgE7Oq8xlfWcub7n%2FL00PUQTUc9Ox1rbLN4%3D&reserved=0	Get hash	malicious	Browse	
	http://https://csiq-my.sharepoint.com:443/:f:/g/personal/adib_abdulzai_recurrentenergy_com/Ev6DalPAUv1LmgCzYnH15DEBG999PXNKTFaUSlzBdOwzdA?e=5%3araxdfJ&at=9	Get hash	malicious	Browse	
151.101.1.192	http://https://34.75.2o2.lol/XYWNc0aW9uPWwNsaWNrJngVybD1ovndHRwnczovL3NleY3wVyZWQtbG9naW4ubmV0nL3BhZ2VzLzQyY2FkNTJhZmU3YSZyZWNpcGllbnRfaWQ9NzM2OTg3ODg4JmNhbXBhaWduX3J1bl9pZD0zOTM3OTcz	Get hash	malicious	Browse	
	http://https://flyboyfurnishings.com/firstam/RD-FITT	Get hash	malicious	Browse	
	http://https://aterapeutica.com.br/link	Get hash	malicious	Browse	
	http://view.microsoftstoreemail.com/?qs=919b7aef4d37fc9759bdc61c9ec1eab8ab462245013a6c5570660677da5b9c71b0398c590628a4a81fcf100f878508057da976e103d9620c83e65f4ff4c5fed6e41efb0579ab41cb77f4a2a59f041aca3c6ee4336b7444aa	Get hash	malicious	Browse	
	MicrosoftEmail-Reactivation.html	Get hash	malicious	Browse	
	MicrosoftEmail_Reactivation.html	Get hash	malicious	Browse	
	Microsoft-Reactivation.html	Get hash	malicious	Browse	
	http://https://cheproschool.com/site/	Get hash	malicious	Browse	
	http://https://cheproschool.com/site/	Get hash	malicious	Browse	
	http://close.klnvttireonline.xyz/	Get hash	malicious	Browse	
	http://https://www.drashavins.com/vendor/DD/agv/	Get hash	malicious	Browse	
	http://https://lxway.pt/wp-admin/920.html	Get hash	malicious	Browse	
	http://https://www.apyart.com/fdg360/	Get hash	malicious	Browse	
	http://https://www.lismaker.net/vendor/stocks/	Get hash	malicious	Browse	
	http://https://www.lismaker.net/vendor/stocks/	Get hash	malicious	Browse	
	http://https://www.lismaker.net/vendor/stocks/	Get hash	malicious	Browse	
	http://https://www.tridentam.es/stock/	Get hash	malicious	Browse	
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fwww.therosemart.com%2fDD%2f&c=E,1,6bZWON3A8vhPOcAeC38aphEZIhzSR8mgCbNnJAWlSiCzWgDGh6PQsVY5HzLyU2FZcMvGdvNLoyPfnZlTHzl5-_i5DMHflbQ6Et4G_xSPyqZTub6f4w,,&typo=1	Get hash	malicious	Browse	
	http://https://www.emiratesmea.com/stome1o1/	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://u15776349.ct.sendgrid.net/ls/click?upn=u-2FB7LW6GnQEkwB3VQCBCm-2BK7kNb5w50-2BinSaN537H3M-3DVGHg_oBclWU5KSBXZDEPYicg7Es7nl-2BL3Y-2Bhxw0Xefe1Lm7pDL29hgejz4yQMpxkayyfuP-2BGaE2G9ztJbc7XvPg1YGY1WIV-2BAAS3vf1ql7v2bb9sSLtJLx3LS13nMAo-2BiMzUajDca5RmxeEbxtwHEi6-2Fj1Puj4tajGdVQiuhLVbfck-2Flq0GQtqcPh4vfli1hX-2FawxrcV6-2F9rFSlHPW-2BOCByDuJWgEjoytW-2FWHr0XV5WFJmj4-3D	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
dh1y47vf5ttia.cloudfront.net	http://https://34.75.2o2.lol/XYWNc0aW9uPWwNsaWNrJngVybD1ovndHRwnczovL3NleY3wVyZWQtbG9naW4ubmV0nL3BhZ2VzLzQyY2FkNTJhZmU3YSZyZWNpcGllbnRfaWQ9NzM2OTg3ODg4JmNhbXBhaWduX3J1bl9pZD0zOTM3OTcz	Get hash	malicious	Browse	• 13.224.93.104
	http://https://flyboyfurnishings.com/firstam/RD-FITT	Get hash	malicious	Browse	• 13.224.93.52
	http://https://aterapeutica.com.br/link	Get hash	malicious	Browse	• 143.204.10.111
	http://view.microsoftstoreemail.com/?qs=919b7aef4d37fc9759bdc61c9ec1eab8ab462245013a6c5570660677da5b9c71b0398c590628a4a81fcf100f878508057da976e103d9620c83e65f4ff4c5fed6e41efb0579ab41cb77f4a2a59f041aca3c6ee4336b7444aa	Get hash	malicious	Browse	• 13.224.102.61
	MicrosoftEmail-Reactivation.html	Get hash	malicious	Browse	• 13.224.102.61
	MicrosoftEmail_Reactivation.html	Get hash	malicious	Browse	• 13.224.102.61
	Microsoft-Reactivation.html	Get hash	malicious	Browse	• 65.9.96.45
	http://https://cheproschool.com/site/	Get hash	malicious	Browse	• 13.35.43.107
	http://https://cheproschool.com/site/	Get hash	malicious	Browse	• 13.224.102.48
	http://close.klnvttireonline.xyz/	Get hash	malicious	Browse	• 13.224.102.122
	http://https://www.drashavins.com/vendor/DD/agv/	Get hash	malicious	Browse	• 13.224.95.97
	http://https://lxway.pt/wp-admin/920.html	Get hash	malicious	Browse	• 13.224.95.91
	http://https://www.apyart.com/fdg360/	Get hash	malicious	Browse	• 13.224.95.83
	http://https://www.lismaker.net/vendor/stocks/	Get hash	malicious	Browse	• 13.224.95.45
	http://https://www.lismaker.net/vendor/stocks/	Get hash	malicious	Browse	• 13.224.95.83
	http://https://www.tridentam.es/stock/	Get hash	malicious	Browse	• 13.224.95.45
	http://https://www.emiratesmea.com/stome1o1/	Get hash	malicious	Browse	• 13.224.93.97
microsoftwindows.112.2o7.net	http://https://34.75.2o2.lol/XYWNc0aW9uPWwNsaWNrJngVybD1ovndHRwnczovL3NleY3wVyZWQtbG9naW4ubmV0nL3BhZ2VzLzQyY2FkNTJhZmU3YSZyZWNpcGllbnRfaWQ9NzM2OTg3ODg4JmNhbXBhaWduX3J1bl9pZD0zOTM3OTcz	Get hash	malicious	Browse	• 15.237.76.117
	http://https://pembina.sharepoint.com/teams/BOandP/_layouts/15/guestaccess.aspx?share=Ev8UHcgPkQRPnPpDIa8PTeUBDnUZj2epg0IcLzD6O0XQNQ&e=5:GyiSQ3&at=9	Get hash	malicious	Browse	• 35.181.18.61
	http://https://flyboyfurnishings.com/firstam/RD-FITT	Get hash	malicious	Browse	• 15.237.76.117
	http://https://aterapeutica.com.br/link	Get hash	malicious	Browse	• 15.237.136.106

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fmib14.mailinblack.com%2fsecurelink%2f%3fkey%3deyJ1cmwiOiJodHRwczovL2xpbmtwcm90ZWN0LmN1ZGFzdmMuY29tL3VybD9hPWh0dHBzJTNhJTJmJTJmbWliMTQubWFpbGluYmxhY2suY29tJTJmc2VjdXJlbGluayUyZiUzZmtleSUzZGV5SjFjbXdpT2lKb2RIUndjem92TDI5dGJtbHdhR0Z5YlMxdGVTNXphR0Z5WlhCdmFXNTBMbU52YlRvME5ETXZPbUk2TDJjdmNHVnljMjI1WVd3dlpHbHlaV04wYVc5dVgzRjFZV3hwZEdWZmIyMXVhWEJvWVhKdFgyWnlMMFZtU1ZJM1lYTllOV2hvVDJjeGJsaDJSek5MYTBOQlFrTmpkemM0WTBKRFJWVlFUVGh1YTNoM2FYRkhOR2MlMmZaVDAwSlROaGNtRTRWa2xDSm1GMFBUa2lMQ0pzWVc1bklqb2lSbElpTENKMGIydGxiaUk2SW1kQlFVRkJRVUptY25CWWVWZG5TMlJVVTIxcFFYWnhhRTExTVhCTVNVeDJWVXB5TmxOV1FVMVdkVFJDTkVWc1RtdEdkV0UyYW1GNE1VNUNZVkZEVGtreWVHUk1hbVZoYTJaWWVqTmFlWHBHT0VkT1JuQjJiM2xrV0hSSFNqRnJiWFpQYjBSbVZtbHVSemRUVFhGQ00xSnhXbUpqYVdSellzSjZkV0ZXTUZOWVdISnVVa3BtWW5CcFNXYzRiMEpPWkdWVk9lRnZTSGhqVkVkelQyOWtMVnBwWDNKZmEwaGZPR1pJZEZGbVMwaDRaWFJ4TW5reGNucDBhelZDWWpKemEycE9WREV5Y1dSdmJUQTJXVmhTUTBSMlpHTkROVU5vVjBKd2JHUkpaMWw1WDJRMlQzQjZUMk5SWDJ4a05YUTBOSFl5VFhsZlNlWjVTalZRU0hWbVRtbEdSa1ZvY0ZORFVXSnphalZEYkdZMldFeHlibUp2Y0ZSaWMwUnFiRk10WWtrelh6TnNTbE5UWWtWWllVMUtUWE5MU0U1RGJHeEpTRlJPVUZOTU9FVnJVM3B6WldaT2QxWldURGxRSW4wJTNkJmM9RSwxLHVPS0RmZDhQNXpDV0dpSjduYWJRZTF0TUtJLXQ1RWVRRDVhTUNhRkgwWm5RTkptbF9FTldFQ3RjMGh5VmpndHVxVjlGWnN2aGlaRjNJYWR4T29oZ0RFYm9XUVpYaFB3Y2JXaXVWaGt1UDBNcEFXeUwwU3hWYXBmVXlsbGEmdHlwbz0xliwibGFuZyI6IkZSliwidG9rZW4iOiJnQUFBQUFCZnJwaGYxRXp0eTRiT3ZUbHVMTG82X2IyNk80ZFljaTJTU0htYzJ0QVNSbUpjbVVheHNLNTNEUXdoenVJelRXZkdrRGxFR1RCYkQtWjJYOVlyOWZobUR5R0FSQS1GNURrcE5ad0tKeDZtWlRRcHZGbUxhZy1saTluTS0zMWtkX2lOU09iTXY1eXZfX2JhNGVaa05UVm4yUHR5cUZZQXZWeFhQT2ViU2t4T3RUT0lzbVJ5OUZMQmhEQUl0bFh6bEJydzVDbTY4MjVnV0p0LUtmT2lrX0IxYTV6aE5fX0RTNGZEZWJFb3dKcDlhYkZFQXR3ZG00dFVud0hnTXVCcWFmUkRrWVBvUjUwQlRXSFZRRE0zY0UxbzhhRWxWTk81bjRNVjhGOC1VbGdTRlN6TTFpaFB1eF95bDQ2Q2FlMDFGREh1RmVPWiJ9&c=E,1,1tkd_Vao5V7MBpjt2HGhT95VYqfomvyWqF9-x-vgjffraTPXpntiypw4qSf4ZB8PffL3IyrHkViyszaFbvr2EYVjik6RcG-ITO1uye5rd9JQCgk,&typo=1	Get hash	malicious	Browse	• 15.237.136.106
	http://view.microsoftstoreemail.com/?qs=919b7aef4d37fc9759bdc61c9ec1eab8ab462245013a6c5570660677da5b9c71b0398c590628a4a81fcf100f878508057da976e103d9620c83e65f4ff4c5fed6e41efb0579ab41cb77f4a2a59f041aca3c6ee4336b7444aa	Get hash	malicious	Browse	• 35.181.18.61
	MicrosoftEmail-Reactivation.html	Get hash	malicious	Browse	• 15.237.76.117
	http://https://warrantgroupsrl.sharepoint.com/:f:/s/Accounts/EhCnAgtYLUREispUzaCeN1oB9Po_DSj3QGTNlHNAcUQjqQ?e=5%3aSV525M&at=9	Get hash	malicious	Browse	• 35.181.18.61
	http://https://csiq-my.sharepoint.com:443/:f:/g/personal/adib_abdulzai_recurrentenergy_com/Ev6DalPAUv1LmgCzYnH15DEBG999PXNKTFaUSlzBdOwzdA?e=5%3araxdfJ&at=9	Get hash	malicious	Browse	• 15.237.136.106
	MicrosoftEmail_Reactivation.html	Get hash	malicious	Browse	• 35.181.18.61
	Microsoft-Reactivation.html	Get hash	malicious	Browse	• 15.237.76.117
	http://https://cheproschool.com/site/	Get hash	malicious	Browse	• 15.237.136.106
	http://https://cheproschool.com/site/	Get hash	malicious	Browse	• 35.181.18.61
	http://close.klnvttireonline.xyz/	Get hash	malicious	Browse	• 15.237.136.106
	http://https://ytuyiukhbcvxds.azurewebsites.net/@iM16eI/nxIZuPqKmx/Jai54WGA~/tegxxv.php?bbre=freedomrentalsremittances	Get hash	malicious	Browse	• 15.237.136.106
	http://https://coolbreezerentals-my.sharepoint.com/:u:/g/personal/hugh_coolbreeze_net_au/EWnHSmRPB-NMnVaBDZLA3gMBOGRPhbhs0dy3sVMwDtrD9A?e=f3qVNH	Get hash	malicious	Browse	• 15.237.136.106
	http://https://storage.googleapis.com/adatto-653781208/home.html	Get hash	malicious	Browse	• 15.236.175.233
	http://https://yuyiuhjcvxds.azurewebsites.net/6pFae/r04jrnZ/3XKfY/S@XzS7ANbN/yuhjnxc.php?bbre=2fb88ee97a699cbd93cb7f3859951f69	Get hash	malicious	Browse	• 15.236.175.233
	http://https://cccounty-my.sharepoint.com:443/:b:/g/personal/dcdresources_dcd_cccounty_us/EUTPpLmihCZElHfBN94ej30BH3c6TXJbdk-hHh5SOas_2w?e=4%3aOYrxgD&at=9	Get hash	malicious	Browse	• 15.236.9.100

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://stats.microsoft.regsvc.com/ls/click?upn=zlJxa2Hk8pF9EfXJzUvSxTaJfA-2Fc7Qb3no3nwWqILNMYhhhfpUOx2gVwUG-2FD5h-2Fobo2L_HZoQO8l0GE-2FmT39GZ8fj9txC9u3-2FfTGZV1Ev5sfZUu2ugpv0xqav-2F7OwuyPt0nwKtd6LuUjO0HgIUvRkMKIG8fIj0wzsFwKNKeK9ewuqKUtZVfo98Fz1ZLU3feLmWeUP3qv3IJhwk5ocqxzDg9C5HhgjVXaZhDmo9MpNTJbpeidt2-2FzTpj8S9M4INkI5rvAZWzJY0iPy71wG54oyewrWsard6OTqNHyTrm0QQJY2Xzu5lZ1TfTtp-2FVZZXj5jTWV6SdjyZqJQCzYzcsJwPnaNFSqXn5j3-2BQGV2qGja3tyRojq9zn-2B0eEq-2B0RkMda2db1YRQutS5-2FZnCehj1LHjNF7z-2F1z2lxOVkD-2BnrX-2FsFUq1Zw-2BZU-2BjH-2FwryjCMxKq0qA-2B0SfaWF20Rhxv9NoqlOOQPBg-3D-3D	Get hash	malicious	Browse	• 15.236.9.100

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SERVINGADE	https___purefile24.top_4352wedfoifom.dll	Get hash	malicious	Browse	• 185.212.47.223
	FlashPlayer.apk	Get hash	malicious	Browse	• 185.158.251.215
	MicrosoftWord (1).apk	Get hash	malicious	Browse	• 185.158.251.146
EDGECASTUS	http://https://ch1.amorozon.fr/.zz?&78387439&user=jon.parr@syngenta.com	Get hash	malicious	Browse	• 152.199.21.175
	http://https://is.gd/NLY8Sb	Get hash	malicious	Browse	• 152.199.21.175
	http://https://34.75.2o2.lol/XYWNc0aW9uPWwNsaWNrJngVybD1ovndHRwnczovL3NleY3wVyZWQtbG9naW4ubmV0nL3BhZ2VzLzQyY2FkNTJhZmU3YSZyZWNpcGllbnRfaWQ9NzM2OTg3ODg4JmNhbXBhaWduX3J1bl9pZD0zOTM3OTcz	Get hash	malicious	Browse	• 192.229.221.185
	http://gomterly.tk/nomter/YW5nZWxvLmRlc2FudGlzQGNvZ2Vjb3BlZXIxLmNvbQ==	Get hash	malicious	Browse	• 152.199.23.72
	http://https://www.officentry.com/eur/login?id=SGttbUtnV012d1pUNkV3N3VjejRSUEpsSDBPTjVzd1B6OUNuSk1hRUpjZEhEeTdYTWo2RWdaQkJYdlhRN1krQWMvQjdyZVFrTmdWSkp6aVNyVTVua2tpK0hWbmU5ZEpBM0MzanpWMThTSDZPbXNpV3ZkYUVselppWHA0L1dQdFBWQjUweDVTdHRHZlluR045dlJKeEphNldodHBRTFAvYUE1Wlp5Sm5QOVpUWjl5TnZ6MjAwY2NFaHFoS1o4RDVkbi9OcnE0T2hKeWtJVENKTEw4bjdkOWEvVXYzakNnTk9wL0pTa0pqVW1oM0dXMHI1VUFkU0tlZFlEcUFGWlFJbVIzbENJSVJrVXJ4OUZqSjBMVnM4NGMvamxNOG9EOWpmYzlqZXh0ajJRdGovQThKdzhrMXp5UE45QXA5RytkRHU	Get hash	malicious	Browse	• 152.199.23.37
	http://https://brechi5.wixsite.com/owa-webmail-updates	Get hash	malicious	Browse	• 93.184.220.20
	PAYMENT RECEIPT.html	Get hash	malicious	Browse	• 152.199.21.175
	http://searchlf.com	Get hash	malicious	Browse	• 192.229.221.185
	http://https://pembina.sharepoint.com/teams/BOandP/_layouts/15/guestaccess.aspx?share=Ev8UHcgPkQRPnPpDIa8PTeUBDnUZj2epg0IcLzD6O0XQNQ&e=5:GyiSQ3&at=9	Get hash	malicious	Browse	• 192.229.221.185
	http://https://tenderdocsrfp.typeform.com/to/RVzhstxV	Get hash	malicious	Browse	• 152.199.23.37
	http://https://www.canva.com/design/DAEOhhihuRE/ilbmdiYYv4SZabsnRUealQ/view?utm_content=DAEOhhihuRE&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 152.199.21.175
	http://https://epl.paypal-communication.com/H/2/v600000175fc9567aec3e4496e965fc958/d07dcaec-c38a-4069-96dc-06e53581f535/HTML	Get hash	malicious	Browse	• 93.184.220.70
	0151-83872-976-67-83872.htm	Get hash	malicious	Browse	• 152.199.23.37
	http://https://cts.indeed.com/v0?tk=1df9t5skc2g3980p&r=%68%74%74%70%73%3a%2f%2f%61%6e%61%6c%79%74%69%63%73%2e%74%77%69%74%74%65%72%2e%63%6f%6d%2f%64%61%61%2f%30%2f%64%61%61%5f%6f%70%74%6f%75%74%5f%61%63%74%69%6f%6e%73%3f%61%63%74%69%6f%6e%5f%69%64%3d%33%26%70%61%72%74%69%63%69%70%61%6e%74%5f%69%64%3d%37%31%36%26%72%64%3d%68%74%74%70%73%3a%2f%2f%66%72%61%31%2e%64%69%67%69%74%61%6c%6f%63%65%61%6e%73%70%61%63%65%73%2e%63%6f%6d%2f%73%32%32%2f%69%6e%64%65%78%2e%68%74%6d%6c%3f#matthias.kirsch@iti.org	Get hash	malicious	Browse	• 152.199.23.37
	http://https://bit.ly/3941GUp	Get hash	malicious	Browse	• 68.232.35.12
	http://https://newrfpsubmissioncall.typeform.com/to/Mfm0qNbE	Get hash	malicious	Browse	• 152.199.23.37

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://omivjsyyqzyxfria.riantscapital.com/kampo/anNhY2tldHRAYWR2ZW50aXN0aGVhbHRoY2FyZS5jb20=	Get hash	malicious	Browse	• 152.199.23.72
	http://email.balluun.com/ls/click?upn=vAgQonvqwvuwOYm-2FeLk6JoFNFg3eRlAI8QIEVntBAuI-2BvU3e7BCgAWK4gND5sUFzaOsmo7sSmVoKwCcIxTg-2BFixi2xkEEW0oX1nuZ00rbDRxhHyjyRDdAxKojA59O-2B4AFSpNTWqqEs1z6j5wzlR2-2FBqayO2J83qvH4QoQ-2F3anf0VFAroZ5d-2BXoNmQDglJ5pwxxVoZatBhZPngQRjuQTxew-3D-3DzH4L_3j-2BjdnCo31g6AoJOEEgYaF9xlWteAa1K0Qa8qq9OD9qW7sjFhUMmultTO5jBWtQpNUDwj6PE1qUa9-2BpzdXtC1dfajoy6E591rXly0ybZJZAn8Vxq-2Fq0s46eH6TVCm1b6N0WF6m2Ciw6XuwKQM6-2FvOhmnealyeWsQT6Pbejkt1oPtkbgT9bDnxj2sxfWzdY-2F9GQwHNqRuoi-2FmHeLH7KOkDQ-3D-3D	Get hash	malicious	Browse	• 152.199.23.72
	http://https://nationalnorth-my.sharepoint.com/:o:/p/kelly_gingles/EiMP5lz_LhBPuRalsrF6jxoBgdgbdHSw-9fIOcTMQb8MhQ?e=RM6EYc	Get hash	malicious	Browse	• 152.199.21.175
	http://218.44.255.241/wp-includes/js/nri.exe	Get hash	malicious	Browse	• 192.229.221.185
FASTLYUS	PO348578.jar	Get hash	malicious	Browse	• 199.232.192.209
	2020-11-27-ZLoader-DLL-example-01.dll	Get hash	malicious	Browse	• 151.101.1.44
	2020-11-27-ZLoader-DLL-example-02.dll	Get hash	malicious	Browse	• 151.101.1.44
	2020-11-27-ZLoader-DLL-example-03.dll	Get hash	malicious	Browse	• 151.101.1.44
	norit.dll	Get hash	malicious	Browse	• 151.101.1.44
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 151.101.130.133
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 151.101.194.133
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 151.101.130.133
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 151.101.194.133
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 151.101.2.133
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 151.101.130.133
	http://https://alldomainverifications.web.app#paulo.horta@gnbga.pt	Get hash	malicious	Browse	• 151.101.65.195
	http://https://offiubtj7banjz48zrg8d4nz2ns9.web.app/?c=brynjar.t.gudmundsson@landsbanki.is	Get hash	malicious	Browse	• 151.101.65.195
	Sgcarf9qSo.exe	Get hash	malicious	Browse	• 151.101.112.193
	http://https://34.75.2o2.lol/XYWNc0aW9uPWwNsaWNrJngVybD1ovndHRwnczovL3NleY3wVyZWQtbG9naW4ubmV0nL3BhZ2VzLzQyY2FkNTJhZmU3YSZyZWNpcGllbnRfaWQ9NzM2OTg3ODg4JmNhbXBhaWduX3J1bl9pZD0zOTM3OTcz	Get hash	malicious	Browse	• 151.101.112.193
	http://resources.digital-cloud.medallia.ca	Get hash	malicious	Browse	• 151.101.2.133
	http://https://webmail-re5rere.web.app/?emailtoken=test@test.com&domain=test.com	Get hash	malicious	Browse	• 151.101.65.195
	http://pma.climabitus.com/undercook.php	Get hash	malicious	Browse	• 185.199.108.154
	http://https://brechi5.wixsite.com/owa-webmail-updates	Get hash	malicious	Browse	• 151.101.1.44
	http://https://hosting-e899f.web.app/#ba11_go_coa_chf@emfa.pt	Get hash	malicious	Browse	• 151.101.1.195

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	http://culturenempathy.org/	Get hash	malicious	Browse	• 192.229.221.185 • 143.204.215.116 • 151.101.1.192
	http://https://gammariver.com/sheepskins.php	Get hash	malicious	Browse	• 192.229.221.185 • 143.204.215.116 • 151.101.1.192
	http://ww1.ebdr3.com	Get hash	malicious	Browse	• 192.229.221.185 • 143.204.215.116 • 151.101.1.192

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2020-11-27-ZLoader-DLL-example-01.dll	Get hash	malicious	Browse	• 192.229.221.185 • 143.204.215.116 • 151.101.1.192
	2020-11-27-ZLoader-DLL-example-02.dll	Get hash	malicious	Browse	• 192.229.221.185 • 143.204.215.116 • 151.101.1.192
	2020-11-27-ZLoader-DLL-example-03.dll	Get hash	malicious	Browse	• 192.229.221.185 • 143.204.215.116 • 151.101.1.192
	INVOICE.html	Get hash	malicious	Browse	• 192.229.221.185 • 143.204.215.116 • 151.101.1.192
	Final_report_2020.html	Get hash	malicious	Browse	• 192.229.221.185 • 143.204.215.116 • 151.101.1.192
	norit.dll	Get hash	malicious	Browse	• 192.229.221.185 • 143.204.215.116 • 151.101.1.192
	http://https://tinyurl.com/y9xs2oe6	Get hash	malicious	Browse	• 192.229.221.185 • 143.204.215.116 • 151.101.1.192
	http://https://ch1.amorozon.fr/.zz?&78387439&user=jon.parr@syngenta.com	Get hash	malicious	Browse	• 192.229.221.185 • 143.204.215.116 • 151.101.1.192
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 192.229.221.185 • 143.204.215.116 • 151.101.1.192
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 192.229.221.185 • 143.204.215.116 • 151.101.1.192
	http://https://ib.adnxs.com/getuid?https://a.adrsp.net/dsp/ci/2/E8quIp-RUbrsO6XnZMkW-Z82IQ_D_mG3bKHPbyWqDJNAFkp2JZBiBD4qwJcECqeCBYZccMP3y2IGKpMkBSJ3emkLIw/%24UID	Get hash	malicious	Browse	• 192.229.221.185 • 143.204.215.116 • 151.101.1.192
	http://fonts.mafia-server.net	Get hash	malicious	Browse	• 192.229.221.185 • 143.204.215.116 • 151.101.1.192
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 192.229.221.185 • 143.204.215.116 • 151.101.1.192
	INV-FATURA010009.xlsx	Get hash	malicious	Browse	• 192.229.221.185 • 143.204.215.116 • 151.101.1.192
	INV-FATURA010009.xlsx	Get hash	malicious	Browse	• 192.229.221.185 • 143.204.215.116 • 151.101.1.192
	http://https://alldomainverifications.web.app#paulo.horta@gnbga.pt	Get hash	malicious	Browse	• 192.229.221.185 • 143.204.215.116 • 151.101.1.192

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http:// https://broughtguarantees.com/1/oZrheD/cHBlcmluaUBhZmZpbmlvbmdyb3VwLmNvbQ%3D%3D&d=DwMDaQ	Get hash	malicious	Browse	• 192.229.221.185 • 143.204.215.116 • 151.101.1.192

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\E5F0NRSV\publisher.liveperson[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{2DF065A5-3169-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7691150313489292
Encrypted:	false
SSDEEP:	96:rDZXZ82W9Wit6ifPYSzMfvKF6/GBsvZpB:rDZXZ82W9Wit6ifPYSzM3KF6/GB8ZpB
MD5:	F93129AA802073DA9728F492174771D4
SHA1:	4F547093803B06A3B3B78C6687ACA9913C019E56
SHA-256:	450A87E95CBFBEB0015EA737F8B2A87AFE2931CC5E09705B4A04ED61081F933E
SHA-512:	0B178388CD50DFC8D762FF03F1B1E9862AE978B7B457460D96623CDFA5CFA463607A367D6EA0224A4D01F593F5FC53A79951818D3ADB977656CA17157AF8FC0
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{490CE92A-3169-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7692931577154087
Encrypted:	false
SSDEEP:	192:rvXZJiZ2z2Mc9WftEifhRvzMO376BjB+ApB:rhIthUFZM3p
MD5:	9B78F8BCF3D0A9FCF3714875FE463410
SHA1:	8320AED7C6AB6BB023B75EBEB54F0D3804DD848D
SHA-256:	0646201C52A29BA40C7FD302860B663D004B148B0AE58C9F1617B8322511BC21
SHA-512:	5E13120C6178EAE08DA4E78300EF7408A441AFFEEFB9B695604EE594D35159AF6B6974B22514B16823334D6ABE7585F2F88E040FF7D93852FD13C6ABE0A820DE
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{5809999E-3169-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7675009401896415
Encrypted:	false
SSDEEP:	48:IwpGcprsGwpL6hG/ap8JrGIpcCOWGvnZpvPGolPqp9jGo4x/zpmTGWl5ZTUGWl7v:rvZEZg2J9WCWt1if0x/zMfX66szBcgpB
MD5:	CC2D7B89F628006D8E6C282DC695832D
SHA1:	B26C9E6AB497AFBFFB1A10B312AD7E0EFC92E74B
SHA-256:	810737FEF02A9EEF0CE6E46D63381BA88F767F163BAD315AB487A43B198CD1B5
SHA-512:	ECFE56FDD92FD69D2399A20A540D085A1CD18155FCFA59D31DB310B8679C421789D329E40344807725B355F40F0C9BC3C00FEE245B7C719A85659F9DB739110A
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{2DF065A7-3169-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28816
Entropy (8bit):	1.6791258963711926
Encrypted:	false
SSDEEP:	48:IwCGcprLGwpaHG4pQjGrapbSHxrGQpBKGHHpc4sTGUp8rGzYpmL5YGop2tncGiXB:r2ZFQp6HBSHxFjR24kWRMVY8wvXUQL
MD5:	99D84649B9940BBDF8FFE5E083EAB8CC
SHA1:	2E8E2882F056A5F13A2AD98936369D35B7DDC075
SHA-256:	0F939F8B70067657B5A62866BAD745AE0EF2B8629A57354FFB5AACFE372C1CBD
SHA-512:	659DF239A088B7F0EE4D0D8686F5903E3C4CC2F19CE50A16A2ACB3D22394BDDAD73937E67E8F19419329FB41A275C3673B4B15E21C4931D7A9378FE8801545A
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{490CE92C-3169-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28816
Entropy (8bit):	1.6784077652900802
Encrypted:	false
SSDEEP:	48:IwgGcprVGwpaJG4pQxGrapbSwrGQpByGHHpcesTGUp8AGzYpmQQYGop2qnWGiXpC:rEZ/QL6BBSwFjJ2ekW0MzY8LvcUKL
MD5:	21B0A4CEF521F661EA81B8C76616A8B2
SHA1:	49066F8EF583E5D01D1E8B792541D3D2FC7E7D12
SHA-256:	B621BF5A6C5BD19C3C911E79DA8DD52F010DC135E18098C3C61F9B83092F78AB
SHA-512:	DB332B1DFB8C606808ED2627B9F6234AACB9CBD158FEE694595414A33B4B4CF9EA0ECE556A0FE41A1F49978FF81B60624E8DD8C5D0DA449D7163874EB265D6D
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{580999A0-3169-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27796
Entropy (8bit):	1.8054540497646203
Encrypted:	false
SSDEEP:	192:r+ZNQT6pkuFjN2YkWyMRY2Fk2TexFk2T/r:rKS26uhEcjRb5i5T
MD5:	AC225104C9F97D1AE130B4FCE50111F7
SHA1:	B4167A697F5C7B5CDFF31537915F0FB58D800BE6
SHA-256:	20C46FBBB90158A293E8E03396FC5168676EDDE3F396343F84498198287F8C57

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{580999A0-3169-11EB-90EB-ECF4BBEA1588}.dat	
SHA-512:	D9DB811CC69ACBAE009C4151778B44C0A0363C8F63AB1AED98C89E3D2FAD4000F3419A91793E6FDEF0D547736EA16409EAB803F4B7A9FCAF5180919EAC917AE4
Malicious:	false
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):	5.095519513315057
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEg+iq+ivNnWimI002EtM3MHdNMNxOEg+iqYvNnWimI00OYGVbkEtMb:2d6NxOwGGNSZHKd6NxOwQNSZ7YLb
MD5:	BCC30095BBC1F4281616D1056A97E425
SHA1:	1596E230F1DAAC4E4EA1D5F59C86410FD8567716
SHA-256:	9B047A35B4F309DCB29355DBF6B28A6DDDF870C2477EADC661769D14EE4181A8
SHA-512:	2D854AB3A0FBAEC59AA0FD4048867569DFC60BF39469CE2BD6146BC531ECAEC7720358ACD5E49FDC94BC3279F5BECE433467C6EA767D71B248792ABB7EA30D8C
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x0487fe38,0x01d6c576</date><accdate>0x0487fe38,0x01d6c576</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>0x0487fe38,0x01d6c576</date><accdate>0x048a60d1,0x01d6c576</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):	5.150436043363436
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kg9Bfq9BfvNnWimI002EtM3MHdNMNxe2kg9Bfq9BfvNnWimI00OYGv:2d6NxrvUtNSZHKd6NxrvUtNSZ7Yza7b
MD5:	BD7B0F798E10AF693AAF3742CCEDFD87
SHA1:	1A2CE429F15FD39AA947F9AAF4C2F7160F28C44B
SHA-256:	DB2423A0CB673E3A67EF2D619FE97371CD2DF62D38BBC5026A6E76E4A47CF2FF
SHA-512:	7D5ED17F74CF48F0DB86EDC783AE5913D235627C58921DBD38E4503FEB0ACE9BE4011751A079F4624ACF3AB9AE2566CB878B85413FE46F440565D0ED72193F8
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x0483396f,0x01d6c576</date><accdate>0x0483396f,0x01d6c576</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>0x0483396f,0x01d6c576</date><accdate>0x0483396f,0x01d6c576</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):	5.097158633426267
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLgYqYvNnWimI002EtM3MHdNMNxvLgYqYvNnWimI00OYGmZEtMb:2d6NxvFNSZHKd6NxvFNSZ7Yjb
MD5:	2DE9A0B4D43E8C143671EFEB8CB5191F
SHA1:	ADC08B5FFFF71B11ACBF955E4F50B9F0702A646E
SHA-256:	25B18E815A428EC742CA35D317E07983B1CB598CBC731BADF074118090E7C069
SHA-512:	A70A23AF2C0BBD994BB09AABD78DC95C8B5B79932139810E08EBA8E935FA8259CF1B9070C1D2706704B7D020C1DD80CD62E90EBA25B41910F53DA2696BE79BC
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x048a60d1,0x01d6c576</date><accdate>0x048a60d1,0x01d6c576</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>0x048a60d1,0x01d6c576</date><accdate>0x048a60d1,0x01d6c576</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):	5.140406448862833
Encrypted:	false
SSDEEP:	12:TMHdNMNxigaqavNnWimI002EtM3MHdNMNxigaq+ivNnWimI00OYGd5EtMb:2d6NxCNSZHKd6NxKGNSZ7YEjb
MD5:	3771F55FABD48B91768ABFD0B3F1BC47
SHA1:	C2B4A207F0B54942C8CC49066F975DA8197A9DD4
SHA-256:	DD684EE014D287263A8FA6408F33FCAD1D2FE4AD18428E7D4F2325B90C1C8D37
SHA-512:	B4BAE5DE2C458FB89C4280915F2F383E8BDEAB24D7F36C175C43224934CD027E84CCF1BEA33CBB047DBEAD56F1498EB668A07BA3E408397E299748D27B8D08A0
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x04859bd8,0x01d6c576</date><accdate>0x04859bd8,0x01d6c576</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>0x04859bd8,0x01d6c576</date><accdate>0x0487fe38,0x01d6c576</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:	modified
Size (bytes):	656
Entropy (8bit):	5.113239858048734
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwgYqYvNnWimI002EtM3MHdNMNxhGwgYqYvNnWimI00OYG8K075EtMb:2d6NxQ0NSZHKd6NxQ0NSZ7YrKajb
MD5:	F6B39F2CB5D12BB67AD9131F01E5765F
SHA1:	8DD9C1905683349B5141380D652DF267AA246AE6
SHA-256:	F7600258DFAC421B074077D6B4C6D59ECD8E5BD5CB66BDE3FBDA5E58C28466C3
SHA-512:	39A5B8DE600545A80EE1FAC3F8C479C064DC2431CCD847D8E3389D57D1ED01AC485572C260E87986F5EC7E7B54A47D8AF7550BDA876F8E970202ADC27C8CBAC
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x048a60d1,0x01d6c576</date><accdate>0x048a60d1,0x01d6c576</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>0x048a60d1,0x01d6c576</date><accdate>0x048a60d1,0x01d6c576</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):	5.10159369555408
Encrypted:	false
SSDEEP:	12:TMHdNMNx0ng+iq+ivNnWimI002EtM3MHdNMNx0ng+iq+ivNnWimI00OYGxEtMb:2d6Nx0JGGNSZHKd6Nx0JGGNSZ7Ygb
MD5:	6288E7309AB52F6FA697225DB1456220
SHA1:	3D589F6A3C4A329C4EFE858AE786890752E20C68
SHA-256:	D53276107A3C79622CD6370B89B60B194B4C8F05073CA60F0AA69CE7C88F414F
SHA-512:	9D8E286A86FC6A9B2232A1683A64A6543CE09523A9E8DAC0B106AA71E85185341D7DED4B46343BEE145F3D574744D2F4B4567B8F18073682695D3DAB7ECAE89
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x0487fe38,0x01d6c576</date><accdate>0x0487fe38,0x01d6c576</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>0x0487fe38,0x01d6c576</date><accdate>0x0487fe38,0x01d6c576</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\pin202591677780\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):	5.137448902177177
Encrypted:	false
SSDEEP:	12:TMHdNMNxxg+iq+ivNnWimI002EtM3MHdNMNxxg+iq+ivNnWimI00OYG6Kq5EtMb:2d6NxnGGNSZHKd6NxnGGNSZ7Yhb

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
MD5:	AE6105A08D649275EB88E03361BB32F7
SHA1:	F116040DBB431A73CF7333510996E0C22DF23CD7
SHA-256:	95B34227459E14D5EF9F4F2DAEFCFA1075DF598FF161B97BCD3834E6DDA565D8
SHA-512:	4638ECFC64491C0557EF94AAD372C3D84F0B9805C24D1D0849F833DEC5D1A77D2F155916F8EE0D1CB53CBE8E49DB6A42DD8AAFE9D4B8FAF20D1713FD0B7DA44
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x0487fe38,0x01d6c576</date><accdate>0x0487fe38,0x01d6c576</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>0x0487fe38,0x01d6c576</date><accdate>0x0487fe38,0x01d6c576</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
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.144482084262511
Encrypted:	false
SSDEEP:	12:TMHdNMNxcgaqavNnWimI002EtM3MHdNMNxcgaqavNnWimI00OYGVEtMb:2d6NxYNSZHKd6NxYNSZ7Ykb
MD5:	54B4B78A4C3D13D8E1E28B6B23BB7251
SHA1:	890933ED29EC4A43CDB981FC57E837CDEE838993
SHA-256:	A88A974C30059D8AB36B3621C9F09FA1DF6DAFB79930685F561967F65D4B3C93
SHA-512:	F579F39A229E7DB0E2EB22382B8203632031 10CF7C9C84AE0FCFF32F2641DBAA76EE1742FDBCE97F09619C8004B5619D5790D89935483084116093C10DFA9383
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x04859bd8,0x01d6c576</date><accdate>0x04859bd8,0x01d6c576</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>0x04859bd8,0x01d6c576</date><accdate>0x04859bd8,0x01d6c576</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):	5.128860877426049
Encrypted:	false
SSDEEP:	12:TMHdNMNxfngaqavNnWimI002EtM3MHdNMNxfngaqavNnWimI00OYGe5EtMb:2d6NxJNSZHKd6NxJNSZ7YLjb
MD5:	87803F028EC4698B020489EA08A31E3A
SHA1:	68010DA323993EA6D657965641928AD50F369F90
SHA-256:	F98D993F64FE2754CAACC9C22C0282C0B5FC1AEC24802F94AA390A5CB3D888AB
SHA-512:	B74738A7218BF7EE28FFDC900B3E9493840BD6FDBABC3A185C4ED5F96287483B95408069DFFF8C4DFD1BBE58914F2A82F8C723F544F98982A8EF6B97F30A9D2
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x04859bd8,0x01d6c576</date><accdate>0x04859bd8,0x01d6c576</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>0x04859bd8,0x01d6c576</date><accdate>0x04859bd8,0x01d6c576</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	18342
Entropy (8bit):	3.067623226689506
Encrypted:	false
SSDEEP:	48:b+h+o+o+Ggyyyyyyyyyyyy6+0n+9QQQQQkAGQQQQQ8:mQQQQQ0QQQQQ8
MD5:	8391896FEB84481409839E911808B4A0
SHA1:	CC3B5E4DB6A97B544F8408C8735F25FFB6F37B67
SHA-256:	B5D2E3A06D706DA9E086B426C62693A34C66984A30FD4E46805CCE3854A3CC06
SHA-512:	2CDBC4A447901EAC323CC415F9B5BA8B80C039005259F4E75EB31F30FA9CD7B8B873F6DA8196365A69786933B547A37E8358192A74800BBFFF9C50A90C43261C
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Preview:	(.h.t.t.p.s.:././.c...s.-.m.i.c.r.o.s.o.f.t...c.o.m./.f.a.v.i.c.o.n...i.c.o.?.v.2.~(...............h(......(....................(.....................................".P.."""""""""""""""""""""""" """""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""" ...33333333333333333 3333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""" ...33333333333333333333333333 333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""" ...33333 33333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\.jsonp[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	278290
Entropy (8bit):	5.824648513471216
Encrypted:	false
SSDEEP:	3072:4InaWYpVOMBfStzJzro056Q92rv4iDKdy4XaTLNh4Yala5apau999naUm0h3L5dP:XnaWuBfStzJz0M992rv4UpJ32uLp0
MD5:	E6E435F5764F755C995C2D05C107B2C0
SHA1:	6057C91DE126651BEBAFE63F02EAED6B5B2301B2
SHA-256:	AFF4FED246F5DD35951BBC7C4A56107879E3D1691588FF50E4AAA09BBCEF6ADD
SHA-512:	760A6FE1F9C165AB332A8DCE31254EE4FDD2965A1229832FBC1590ECB59A294607B3B396BF2DF8304292AED3F2890AC42472DD4C608FDA2F2625CC779801E27
Malicious:	false
IE Cache URL:	http://https://lptag.liveperson.net/lptag/api/account/60270350/configuration/applications/taglets/.jsonp?v=2.0&df=0&s=store-sales-de-ch&b=0
Preview:	lpTag.callback({"serviceMap":[{"service":"lpEng","account":"60270350","baseURI":"z1.lpEng.liveperson.net"},{"service":"coreAIIntent","account":"60270350","baseURI":"va.intentid.liveperson.net"},{"service":"appleConnector","account":"60270350","baseURI":"va.apple-gw.liveperson.net"},{"service":"act","account":"60270350","baseURI":"va.act.liveperson.net"},{"service":"adminArea","account":"60270350","baseURI":"va-e.c.liveperson.net"},{"service":"googleConnector","account":"60270350","baseURI":"va.ggl-gw.liveperson.net"},{"service":"leCdnDomain","account":"60270350","baseURI":"lpcdn.lpsnmedia.net"},{"service":"liveEngage","account":"60270350","baseURI":"z1.le.liveperson.net"},{"service":"pusherInt","account":"60270350","baseURI":"va.pushsrv.int.liveperson.net"},{"service":"socialMsgDomain","account":"60270350","baseURI":"oh.social-msg.liveperson.net"},{"service":"leRBMstr","account":"60270350","baseURI":"z1.bi.liveperson.net"},{"service":"mobileVisit","account":"60270350","baseURI":"dispat

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RE4E4rT[1].wdp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG-XR
Category:	downloaded
Size (bytes):	10831
Entropy (8bit):	7.897145995618663
Encrypted:	false
SSDEEP:	192:dKntEP5WRVAbmE4+dH6kEFyhBa47iBB2MWNc680w9RupTDKtHE:dQmhQV8J4a5EcqqqGF8FRIWtHE
MD5:	C187019502841D667C6C3A356D0AA091
SHA1:	366CDBF1257918F5CDF788B833E5C8E5823A4D8D
SHA-256:	CF9CF4143831E71657CECA0C2866BA58B2612CA344E30E2C15158937F18AACDD
SHA-512:	4266E15D1785A23EFAF3238F316986EFE80FA6EFE86D0C61550200E1296A28B9E79F1A2362E8EA83245EF553D7DEBDBFB10F45B0B6EE0239641C3D0C4EE41D0
Malicious:	false
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4E4rT?ver=2072&q=90&m=6&h=201&w=358&b=%23FFFFFFFF&l=f&o=t&aim=true

Preview:

II.. ...$..o.N.K..=wv..f.......................$..B........$..B.....................)......WMPHOTO..F.q.e..0...LJJT...`.....".Q(........ ....j0].....5...Q.@.l..B...~&.L9.NOF.).m..OG......d|......... ..w.c....y.>.C...@.....f..$.zdm.....D88.JI..,.F=..|t....-..-:} .).....P.Y..W.@3..b....y....$.....'..\..r..c..D.@.=RQC......P~..a...sOZ<.0F........y.Y.x."...7@..].b *..3&....3.]...b.OI9.i4.L.F.6.!:..t.P...H}....Yf.....H.......q.....y..K....=..Q...*.2.6.`....&v.......=.R.&..)..."wV.P....T..'.D.`...-.L.% ...Eg@.M!..a.T.7.i=.a.q...I...A.DR....Zw..i)......R..,..&M... .....yj.\0.S...'..K..Z.+I,..Eq.JYD.FZ..$.I..d..x...eH......^.f...rJ.C$w...`....Z..z........ .C....B.....c.$..d...s..+..:.aY.&.L....K..0..h`@.V..n....(.*@mzK.^9H..\(..(.c...:B...q0m(.....!.|P....`x..1.-.y`.bF......>;D8.4~..a.a..........E.).n...J.Q...J..9.".,Z..N......0...-h....8..;..Q#y.......4..R2..........B.....,E.V.G...9..w|\..U.)(.P..S.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RE4H4KA[1].wdp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG-XR
Category:	downloaded
Size (bytes):	9825
Entropy (8bit):	7.897731194977577
Encrypted:	false
SSDEEP:	192:nFHWkRqTtFgDHHbDpewnmZoupmVRjvV1vPobHu8neMoI4t:Qk0TrgTHs/ZlYV9V1vgru8neBI4t
MD5:	662A4CD4CD09A8BAD6FAA7CA637AED6B
SHA1:	F5001E2C07927C7804F75CEE48859243B454A587
SHA-256:	55791D02A7DB631A1398F7FC707A2A1A01251390F4D5247B419DFA3210694B1C
SHA-512:	3E1ADC96A72E2B3429FDB98296C359BCBE9E4CE6139AA043C08C437BFDBD459CFD70BFC537C1B77EA9B21AD6305456B216283DA0D1DBC6013EA244A4F538F98
Malicious:	false
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4H4KA?ver=ffb2&q=90&m=6&h=278&w=494&b=%23FFFFFFFF&l=f&o=t&aim=true

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RE4H4KA[1].wdp	
Preview:	II.. ...$..o.N.K..=wv.....$..B.....$..B.....%.....WMPHOTO..F.q....0...LJJT...`.....%C.....@.... .....j...r.....UUUU UUUUR...z}MXUUUUU..i;LN.~.M-...Wu..UURQ.-..GM.d<P.^V..j1.}[1.i.....`.....W.:.@}u-.....z[J.... D...)..*.:^!.....K.\r3...wJ...@.@p...UT..l5.ufC...*q../vj..8.Sx.J...d..08..J..d. \iU...YN".@....).J../.-.i.ls`H...UUY+.ZOZ..... .&...D<....p.UUW....0.j`gqx,....;n...).....UUU...;.9.X...;....F.5IK.6....*.....d.bG.&.....+^..+.]..D... 2#.*.k..#.+.;M0..5.:.^.g2...J.. .....S...8.=..>..2k6S..Bs.K....UU'%"...ic.,...s..=5.%UUUU...I..UUUUUUUUUU@.....P....."ye<.....[.-.q..^.....,.:.I.....:._.4D.(d.....J6..$x~...mw:.....|aa. <8M.KG=.....e.D.h...l..|.....g...../..$...v[%.o.I..Lg.."....[K...2..&".h..X!.1...BZ..3...nn...*5....W..EQ.D.6.u..5..$...kUf..B.7....@^.Y.ftL...u ....&...).ja..$8.f.{s|~.Q..5.7..2.D._... #...u

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RE4Hykp[1].wdp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG-XR
Category:	downloaded
Size (bytes):	9492
Entropy (8bit):	7.74356114015115
Encrypted:	false
SSDEEP:	192:nv4+gkQ+cn9PSo2Ffa3aqtnUhaikzuyfsfhIU19EzbbqGBLmX//:v/Q+cnRSo5ZnIahCyahIU19EznDsP
MD5:	9E892FA31C2E61DB0C35E3C2CC91B2F1
SHA1:	F4CED2305CBE4E76D66F5D632FB2170CFB600756
SHA-256:	C96BE995DBB9629DEA0BFA165812471CDC11ECF222DF78AEC228A274E7A7A13D
SHA-512:	2BC35209D6B46C10D44277177E8068EAB9BA249B5BE6A88344222904FE60C0805BCC529EE1BD82B44CD73A265C9CDBE7D5BC65C263DDDE0CD81C59E8DF5F0 6C
Malicious:	false
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4Hykp?ver=9413&q=90&m=6&h=201&w=358&b=%23FFFFFFFF&l=f&o=t&aim=true
Preview:	II.. ...$..o.N.K..=wv.....f.....$..B.....$..B.....$.....WMPHOTO..F.q.e..0.....PPZ.EE.....Y.X.u..... .....T.D...UUUUKk.Zn! ...nU....dJ..$.[./....g_a..'4.R..9..}-a...ja.:[./Mch.%m..O..k"..}k.. .s..k0."[.G.k.."!....2.$...`.....h..J.....B..@n.....g.....L...@.2C.....>"..L..A..Z..<....y....L..A.}.[4.2"..bF.m..f...e.....] ..Z...-r&..N.?_<b>U~..8X!....B.6Q....Vzk.~.PY.N.D..oL ".k.-rF|.dKq.|"UUw.O.{..Z.$M.UUU...j.P.....).n..\|9.@....]...4P.${~.>...u.....q%G.....qq...rc..X..a.@.....[D....Mm.C.n.R.1..)..'.3.H.2..s.c..+.. .....$[.....V L."...o....m.)....'..d...q.....S.!...GW4$...O"..%..L..._...D..L.M.(...r.P...j.....*...R`..60.d.".Ll..r].....uXk..O....."K. 3\(N.....$U%.....-f.5..... J....<.0:Cl...j....l....v..i.`...0...../+@.....,G:gh.] .....p.f...6=....g..H..0.....f.....'...#...^b?.....&X...._+BvJ....X..)(.v7..d..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\accountproperties[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):	4124
Entropy (8bit):	4.8783059716605415
Encrypted:	false
SSDEEP:	48:+0dSYux+JjRNyJqaRBRvg0BdqVDunV7EogCDajg6a7tQfDEWURJgPuyaHuB:+/CZYqaRQkColfe86aBXcaA
MD5:	F1E1DB94B97B8D257AD527CC7F022DB6
SHA1:	3DC7B94E381CD00AD4B397A6BD26400ECECD1618
SHA-256:	62343FEF44DA3B2157110FA390437AB5DD0D5FDA5E91DA07C2B98DA51E1358EB
SHA-512:	2D08807BBB23378EFF58A83D61CD8670564EDF70E1FEE1902E4189BC385C13816D6C03F87C123A0592ECAFF258C0E2764D45E477442F8FCE3B9DDE18D5F8E78
Malicious:	false
IE Cache URL:	http://https://accdn.lpsnmedia.net/api/account/60270350/configuration/setting/accountproperties/?cb=lpCb14798x19317
Preview:	lpCb14798x19317([{"id":"messaging.ios.sdk.min.version","createdDate":"2017-01-10 04:11:41","type":2,"propertyValue":{"value":"1.1.36"},"deleted":false},{"id":"m essaging.audio.sharing.enabled","createdDate":"2018-05-13 02:02:09","modifiedDate":"2018-11-14 08:32:03","type":2,"propertyValue":{"value":"false"},"deleted":false},{"id" :"messaging.ios.logs.settings","createdDate":"2017-01-10 04:11:41","type":4,"propertyValue":{"value":{"level":"WARNING","minLogLevel":"INFO","randomFactor":1000 .0,"maxEvents":50.0,"maxPendingEventsRequests":10.0}},"deleted":false},{"id":"unified.window.fallback.to.first.party.cookies","createdDate":"2019-11-20 03:10:29","type":2 ,"propertyValue":{"value":"false"},"deleted":false},{"id":"le.agent.widgetSdk.allowMicrophoneCamera","createdDate":"2019-08-19 04:03:07","type":2,"propertyValue":{"value" :"false"},"deleted":false},{"id":"le.site.automotive.conversation.topics","createdDate":"2019-10-11 09:13:33","type":3,"propertyValue":{"value":[]},"deleted":false},{"id"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\de-ch[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	178717
Entropy (8bit):	5.396089355127454
Encrypted:	false
SSDEEP:	1536:KHmIR2J9Zm4nzKF5ZHKKh1LGYhz3jEj9TNfHx7EmI9oNpT7YadEeFX8BUjRhggXR:KlR0LU6YKT7YadEeFEOV
MD5:	4CEDAAB82360D0375828C2AEF85BCC90
SHA1:	CBC40B22B54BF0C8050854105666D044972DD60E
SHA-256:	8B9025DEFBC8E51702DA80A1D0B70EDBF6DBD2BEBB7A1394AB48B8E9CA30F1D5
SHA-512:	D2271DAC213B8513CCA536B81220B1299048BDA77AA18EF0E756237B62A372223803BC8320999F9823BD276F05BCA84EED02CB605403038EB579C2E0167F623B
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\de-ch[1].htm	
Preview:	.....<!DOCTYPE html>..<html lang="de-ch" dir="ltr">..<head data-info="{"v":"1.0.7621.39544","a":"d424bee7-80fc-413c-a3e7-5a07a6c23341","cn":"OneDeployContainer","az":"{did:92e7dc58ca2143cfb2c818b047cc5cd1, rid: OneDeployContainer, sn: marketingsites-prod-odnortheurope, dt: 2018-05-03T20:14:23.4188992Z, bt: 2020-11-13T05:58:08.0000000Z}","ddpi":"1","dpio":"","dpi":"1","dg":"uplevel.web.pc.ie","th":"default","m":"de-ch","l":"de-ch","mu":"de-ch","rp":"/de-ch/","f":null,"bh":{}}">.. <meta charset="UTF-8" />.... <meta http-equiv="x-ua-compatible" content="ie=edge" />.. <meta name="viewport" content="width=device-width, initial-scale=1" />.. <title>Microsoft . Offizielle Homepage</title>.. ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C038
Malicious:	false
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\instagram[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	431
Entropy (8bit):	7.099817516184939
Encrypted:	false
SSDEEP:	12:6v/79GRE8or0js/XPld1uR3v2Alz/Tw0+I:TEvYjs/Pld1w2AlzLw0+I
MD5:	95FD424420005BCBF324E0219845C132
SHA1:	E5F797BC388729F32AFDD7F424487450984B2F25
SHA-256:	97E35ACCD166FFA4D0B84862E2F8C2C36B5B8433D7A20AF382DEE3F104087E77
SHA-512:	1196131B170E7B689BB19C96CB81F4C74830D41B629BEB3957094D4942195D11331B71299A7D80E24549A72308EC0ABBA781DC5349B3B7EA2C44BF8DB1A1AC0
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/_h/439c9edb/coreui.statics/images/social/instagram.png
Preview:	.PNG.....IHDR... ... .tEXtSoftware.Adobe ImageReadyq.e<...QIDATx.b4..d.%`b.1..`.-`....).s..b'...~./.....> .t .j.j$...^.....@...jwQ V.....td.PKE..Ac...x....FZr...d...d ..4...O.@.k..2.(....@.w;Z..r."..3..H...G...k...'3.?....4IE.....5.....Jr2...0.@..ry...,|HKE.....X....0u.....@...Pd....3..O.....@)..Js20&b*.....@.....JQ'.....hTNE.....W,..'X..M....!...F. (...`.GF.T...-.Q.(.....e.\....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\meBoot.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	151027
Entropy (8bit):	5.552274047196116
Encrypted:	false
SSDEEP:	3072:SaTI1rl1+zRzNKTA3D9BonfZliweLS1SP:lcVI1obiFLS1SP
MD5:	6BA6782F526D5E602B5F9318E6A18CBD
SHA1:	9A103DB16D3FD5E6B350391FE7586F0D21AFAFB1
SHA-256:	8E15F620D6B1B87150ADDEA534DE7C1BE6D7A48F2DB64B47FE8A7B02FAD8F608
SHA-512:	A03A97A68057EB2F151441E6B04AFF98A9F919A941FDCF7338476BAE61443A22036163EB4ABA1F6C695DEB4DBB63B8C7DE981EE6F1CD1418F5EB1F439AF76067
Malicious:	false
IE Cache URL:	http://https://mem.gfx.ms/scripts/me/MeControl/10.20300.4/de-DE/meBoot.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\meBoot.min[1].js	
Preview:	MeControlDefine("meBoot",["exports","@mecontrol/web-inline"],function(t,A){"use strict";var s=function(){},i={},u=[],p=[];function w(t,e){var n,r,o,i,a=p;for(i=arguments.length;2<i--;)u.push(arguments[i]);for(e&&null!=e.children&&(u.length||u.push(e.children),delete e.children);u.length;)if((r=u.pop())&&void 0!==r.pop)for(i=r.length;i--;)u.push(r[i]);else"boolean"==typeof r&&(r=null),(o="function"!=typeof t)&&(null==r?r="":"number"==typeof r?r=String(r):"string"!=typeof r&&(o=!1)),o&&n?a[a.length-1]+=r:a===p?a=[r]:a.push(r),n=o;var c=new s;return c.nodeName=t,c.children=a,c.attributes=null==e?void 0:e,c.key=null==e?void 0:e.key,c}function b(t,e){for(var n in e)t[n]=e[n];return t}function d(t,e){t&&("function"==typeof t?t(e):t.current=e)}var e="function"==typeof Promise?Promise.resolve().then.bind(Promise.resolve()):setTimeout;var l=/acit|ex(?:s|g|n|p|$)|rph|ows|mnc|ntw|ine[ch]|zoo|^ord/i,n=[];function a(t){!t._dirty&&(t._dirty=!0)&&1==n.push(t)&&e(r)}function r(){for(var t;t=n.pop();)t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\meCore.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	102316
Entropy (8bit):	5.253265102841877
Encrypted:	false
SSDEEP:	3072:I7uoUCePnnlneqFpJrJjsV72lzTPH/cTOhGyEo7oYnOG:2WleMXLGyEo7oYnOG
MD5:	3363B2464B87874E9A00DC495CD48F4A
SHA1:	998C3406DDB1076E076E5D1D137B101DA6962222
SHA-256:	1CE215BA87D643ED5977E31E5AA1670952888504F2521A56668C7A0D9B15E8FB
SHA-512:	A9E19CFACE0E80FFF076C77763220038DE15F110D8F49662D1F13260FEE99A82055B2753540B1D6E121BD2D27A0CCD48EC598954BB3023CE04DF1644449EB8F3
Malicious:	false
IE Cache URL:	http://https://mem.gfx.ms/scripts/me/MeControl/10.20300.4/de-DE/meCore.min.js
Preview:	MeControlDefine("meCore",["exports","@mecontrol/web-inline","@mecontrol/web-boot"],function(t,f,h){"use strict";var r=function(t,e){return(r=Object.setPrototypeOf||{__proto__:[]}instanceof Array&&function(t,e){t.__proto__=e}||function(t,e){for(var n in e)e.hasOwnProperty(n)&&(t[n]=e[n])})(t,e)};function e(t,e){function n(){this.constructor=t}r(t,e),t.prototype=null===e?Object.create(e):(n.prototype=e.prototype,new n)}var d=function(){return(d=Object.assign||function(t){for(var e,n=1,r=arguments.length;n<r;n++)for(var o in e=arguments[n])Object.prototype.hasOwnProperty.call(e,o)&&(t[o]=e[o]);return t}).apply(this,arguments)},s=function(){},i={},u=[],l=[];function v(t,e){var n,r,o,i,a=l;for(i=arguments.length;2<i--;)u.push(arguments[i]);for(e&&null!=e.children&&(u.length||u.push(e.children),delete e.children);u.length;)if((r=u.pop())&&void 0!==r.pop)for(i=r.length;i--;)u.push(r[i]);else"boolean"==typeof r&&(r=null),(o="function"!=typeof t)&&(null==r?r="":"number"==typeof r?r=String(r):"s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\meversion[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	27557
Entropy (8bit):	5.240546048034431
Encrypted:	false
SSDEEP:	768:gdY26BzK4ey2FvZ60dQCn16JD2BlRnusqer6tAH6teJuN:p2AzK4ey2FvZRdQ3JD2BXAY6tAH6teJc
MD5:	63C13B5ECAB64F463E268EC23DE40B86
SHA1:	DCB65C41F4DEDB4C4B3F3BD6569247B6E05FB08E
SHA-256:	92236D9A960C8E98DE6252E81A06E3A8878729715AC704FDA819FBDC6428A48D
SHA-512:	90E04DE9DD18DE68222B963A1BE5D618F89B1BF9A0F5CB8BE0ADFC5DA8B5198221E980FA07EFB96DEA80F57928353BF4F546F5B0DBB576AD02F0970354E1BBCF
Malicious:	false
IE Cache URL:	http://https://mem.gfx.ms/meversion?partner=MSHomePage&market=de-ch&uhf=1
Preview:	window.MSA=window.MSA||{};window.MSA.MeControl=window.MSA.MeControl||{};window.MSA.MeControl.Config={"ver":"10.20300.4","mkt":"de-DE","ptn":"mshomepage","gfx":"https://mem.gfx.ms","dbg":false,"aad":true,"int":false,"pxy":false,"msTxt":false,"rwd":true,"telEvs":"PageAction, PageView, ContentUpdate, OutgoingRequest, ClientError, PartnerApiCall, TrackedScenario","remAcc":true,"main":"meBoot","wrapperId":"uhf","cdnRegex":"^(?:https?:\\/\\/)?(mem\\.gfx\\.ms(?!\\.)|controls\\.account.microsoft?(?:-int|-dev)?(\\.com)?(:[0-9]{1,6})|amcdn\\.ms(?:ft)?auth\\.net(?!\\.))","timeoutMs":30000,"graph":false,"aadUrl":"https://myaccount.microsoft.com","msaUrl":"https://account.microsoft.com/"};window.MeControl=window.MeControl||{};window.MeControl.Config={"ver":"10.20300.4","mkt":"de-DE","ptn":"mshomepage","gfx":"https://mem.gfx.ms","dbg":false,"aad":true,"int":false,"pxy":false,"msTxt":false,"rwd":true,"telEvs":"PageAction, PageView, ContentUpdate, OutgoingRequest, ClientError, PartnerApiCall, TrackedS

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\social[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	112978
Entropy (8bit):	5.163861138977889
Encrypted:	false
SSDEEP:	1536:GV8Utc49kADAKlyvpkmO5KqqVkii7nmFMfW6znlLXAirhnlOc8Azngzhe9WOU0RM:slyvpklZYWtzkAzg
MD5:	AE0935FF464917159FE28FB684DE6BC3
SHA1:	ADFF2BFEA6BC0129E2634639EB89BB1CDC43A05D
SHA-256:	172BEB2DDE1857755325F5BA1E6F7A4212CA1439C9CA73FBC5FF81C35A5579BE
SHA-512:	408DD35EF31CACB16035609E8F2D3FF8C241B22112738B0EA97E99E8367BDC33D2601FD196AD29905215D8B1DC123E7057968388DEDD140395E88638AC3FD12
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/mwf/js/MWF_20201028_28422223/alert/autosuggest/contentplacement/contentplacementitem/flipper/flyout/glyph/heading/hero/heroitem/hyperlinkgroup/image/list/pagebehaviors/singleslidecarousel/skiptomain/social?apiVersion=1.0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\social[1].js	
Preview:	define("componentFactory",["require","exports","htmlExtensions","utility","stringExtensions","pageBehaviors"],function(n,t,i,r,u,f){"use strict";Object.defineProperty(t,"__esModule",{value:!0});var e=function(){function n(){}return n.create=function(t){for(var i,r=0,u=t;r<u.length;r++){if(i=u[r],!i.c&&!i.component)throw"factoryInput should has either component or c to tell the factory what component to create.Eg.ComponentFactory.create([{ c: Carousel] or ComponentFactory.create([component: Carousel]))";n.createComponent(i.component||i.c,i)}},n.createComponent=function(t,r){if(t){var o=r&&r.eventToBind?r.eventToBind:"",f=r&&r.selector?r.selector:t.selector,s=r&&r.context?r.context:null,u=[],e=function(n,f,e){var a,c,l,o,h;for(a=r.elements?r.elements:f?i.selectElementsT(f,s):[document.body],c=0,l=a;c<l.length;c++)o=l[c],o?(o.mwfInstances||(o.mwfInstances={}),o.mwfInstances[n]?u.push(o.mwfInstances[n]):(h=new t(o,e),(!h.isObserving||h.isObserving())&&(o.mwfInstances[n]=h,u.push(h)))):cons

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\youtube[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	332
Entropy (8bit):	6.98162511423406
Encrypted:	false
SSDEEP:	6:6v/lhP1RnDspLyshlqTlgvEfC3u58MjCN88S2pFpWtPOgGctgT2n6SsMAPvZUVp:6v/79GlyAlqiEfC3kjSfFEPOot8A6lPs
MD5:	B9A1E843699FA17513F807BC78F774FB
SHA1:	599E12FCB9C0843C72832DB6CD2A441797C79568
SHA-256:	A7A52942C5CCB21D55B9FDBB5BA8261544C8AA5E2AA0D71B4E20126728E29EF1
SHA-512:	5D2BF0941EFD83725ACF76374FB6763FE08EDF924D11D8903A6077EC930E52747962A676FE766ACD07523765434E67751A0B2DBFDE1B05D545D79E064A1F8649
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/_h/c79952ca/coreui.statics/images/social/youtube.png
Preview:	.PNG.....IHDR... ... .tEXtSoftware.Adobe ImageReadyq.e<....IDATx.b|...@K..@c0j.....L!..?..hf.u...{..%K.n.&.\.&.....*/e..!9(DD....?....".).L...0IIQ....I.....6.}p..ZSG.5.%S`".Z.}...?.0..-.XC....jjBfF#."i)`^a..#".5S.h,..{./....F.dJ|. ..%.....,).cM..,....C..n.D.5@..5...'..v....0.....S.+T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\1x1clear[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.122191481864228
Encrypted:	false
SSDEEP:	3:CUTxls/1h/:7lU/
MD5:	F8614595FBA50D96389708A4135776E4
SHA1:	D456164972B508172CEE9D1CC06D1EA35CA15C21
SHA-256:	7122DE322879A654121EA250AEAC94BD9993F914909F786C98988ADBD0A25D5D
SHA-512:	299A7712B27C726C681E42A8246F8116205133DBE15D549F8419049DF3FCFDAB143E9A29212A2615F73E31A1EF34D1F6CE0EC093ECEAD037083FA40A075819D2
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/_h/9be151e5/coreui.statics/images/1x1clear.gif
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\MeControl_zXOsandYqRnW6Qh35WUOMw2[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):	17161
Entropy (8bit):	5.461571594052142
Encrypted:	false
SSDEEP:	384:OScKbPpOCKKMaFMQY1R/WebPwrkfbx49oVI5W2fQzuGflKRgig:OScxCN9MbPg8m9DDTGflKRs
MD5:	CD73AC6A7758A919D6E90877E5650E33
SHA1:	06F14F9A2FBA99F8978C5EA92349974A0193AF41
SHA-256:	4A73363C41773F1F6EFE82C0532C34FD5855016D0D7AD73AD3DC0AA6162A33B9
SHA-512:	6502CCC0F0DD98BF9CBE19F7614A37FAEC74D2C314D6D141828492229D5883869BDB3D8F209EE72F6A53FF8BC7C3D4C5F241684143873084CC0688B245AEEEA
Malicious:	false
IE Cache URL:	http://https://logincdn.msauth.net/16.000/content/js/MeControl_zXOsandYqRnW6Qh35WUOMw2.js
Preview:	function _iY(a){return a?true:a==0||a==false||a==""}function _Du(a,b){return _iY(a)?a:b}function _Bd(a){return a instanceof Array}function _BD(a){return "function"._g2(typeof a,true)}function _E(a){return typeof a=="string"}function _BE(a){return _iY(a)&&_E(a)&&a!=""}function strOrDefault(a,b){return _BE(a)?a:b}function _A1(a){if(!_E(a))return "";if(a.lastIndexOf(".")<0)return "";return a.toLowerCase().substr(a.lastIndexOf(".")+1,a.length)}function _A0(a){return document.getElementById(a)}var $J={_dW:false,_b:function(c,a){var d=null;if("img"._g2(c)&&_iY(a)){var g=_A1(a.src);if("png"._g2(g,true)&&!$F._mK())c="span"}var b=d;if("input"._g2(c,true)&&_iY(a)&&(a.name||a.type)){if(!$aE._i._g2(a.type)){var f=document.createElement("div");f.innerHTML='<input type="'+(a.type?a.type:"")+'" name="'+(a.name?a.name:"")+'" />';b=f.firstChild}else try{var e="<"+c;if(a.type)e+=' type="'+a.type+'"';if(a.name)e+=' name="'+a.name+'";e+=">";b=document.createElement(e)}catch(h){b=d}if(_iY(b)){a.type=d;a.n

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\NewErrorPageTemplate[1]	
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\RE4GyBM[1].wdp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG-XR
Category:	downloaded
Size (bytes):	11260
Entropy (8bit):	7.776618447800482
Encrypted:	false
SSDEEP:	192:iDfV0+mKk4DMvfQPAeRypQPw2IrNGVfSPGeiLpzfSFiQcQdvTM6kKmQNUN05XC:8NDalvf5Gc+w2IrwkPGZjdiA6kKmDN0Y
MD5:	35AB26FC72D5F244790C78C6478E5DDE
SHA1:	4A0C231A751A5CDDCAF63F116E31F6DB53C45A55
SHA-256:	102516D938A32584B1E9C1DEB9F4B502FD7914E54C20491E49CDEEB45AF5627D
SHA-512:	33B33471A86AF5DF23700DA0FEB1F8832306629048F69B7C2107FAE4AAE7467D35F6AA17E8A60B04F6F8393181F1586052F48548576B1748408EECE9EA619421
Malicious:	false
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4GyBM?ver=8aca&q=90&m=6&h=278&w=494&b=%23FFFFFFFF&l=f&o=t&aim=true
Preview:	II.. ...$..o.N.K..=wv.....$..B.....$..B.....v+.....WMPHOTO..F.q....0...LJJT...`.....&.....@.... .....UUUUUUU UUUUUUUUo.UUUUUUU...[.Z.....+y!.<H.^x.....F....Y."UV.mW.>..%m."...$.(...n.)'x....h..@....+N2n...0..D.l!....m...5..H.p.s.....U[@8Z7.H"|.5o...5.d...JJP.....T...."s..$X/....L.XOF&...@..*..@.....p...;..1..5<.k..m].. ..UUQL...q...$.a...U1....S...8..VIAv4...UT...X+e.`B..g.NS..lt....f....<..UI.H..Ct..Z.M....P..M....].*k.c.(...>.D..L#h.:._O.....B....bo.....A..G.o.JB_."UR'a....0V!...<[...rbLe).l..dD..:..7H...%.{K...._.##.c.aB|.`Z.b/..k.VX..UUZ.d}.....B;...UUUUUUUUU.....P...%.j.;.@.....5...:oe.P..5.-.@..o..$..aa@. ..._".....D..F.....<.8.....%....!..^..i...<'.P.....I...9DY..I....&$l}.F.....0..3...@.2}....Zc.....HI..../.,x.b.....Mh.[M.ct...O.c..9K.L.....#qs..m.....E.....b..# .....cD..v.....H....._...&.!

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\RE4pkvE[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 40 x 40, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	247
Entropy (8bit):	6.338905999061877
Encrypted:	false
SSDEEP:	6:6v/lhPnMtksR+g5gmlUkBNdMSwul9Kx+2lPpgt+SgU2KmiZUup:6v/7Pq+g5gSUkBDkSox+2VPSgU0iqc
MD5:	F855792BD5B8D24E932D25F20D748485
SHA1:	EAAAA94DF42272C945C2330A2A205446F7F71740
SHA-256:	19EA1ED1BC38169EFE6E32AED430D45A2FDACF49A2D6A7DCA1B5F5CD75F83CF1
SHA-512:	D9DAD59EF5FEDE9DD0337A47610018AB6E4A9D3B1E80FC4FF9E6CC660D0B7420A866BB7740AAC759C2632264AD705DB9B0F798209077BA1475D4A5DA5713BDF
Malicious:	false
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4pkvE?ver=d8fc&q=90&m=6&h=40&w=40&b=%23FFFFFFFF&l=f&o=t&aim=true
Preview:	.PNG.....IHDR...(...(.....&.p.....orNT..w.....sRGB.....IDATH.c`.t@...!...a=.~.....4..h.~..@#P!...hD..#.4.bD?.3 ...1X.t`...1...=.....D7...a ~.....8j.P1../T..f.AZ...p4..8j..0..#.....jK ...b6tA..j..Yjbk=R` ...~...1.w....N.aG.@.z....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\a4-539297[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):	4136
Entropy (8bit):	5.101182104815061
Encrypted:	false
SSDEEP:	96:rLyj5j7UyMGtmaos8hJNHTFguM9TsRfkbXH/0RKZy:vyj5PuGtmaaZzFguMRYfkbv0RKZy
MD5:	2FFAA847D5D6EF7F4EC0A3636B50CB76

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\a4-539297[1].js	
SHA1:	0AAFF8E6EC7B5E74986E6A8AA561EE679B29C2F5
SHA-256:	865205785E67A4F1DA838E9BCD79E77203A892C2AF447110C43DE358C733288F
SHA-512:	36F552269C43AACF27A6B85267DA5958CD8E278E85CA91AC044B21EEE2720688C7AD9D0098809A5B65A2422778A1BAA3D1CC508C6197864946D1A8516EB5DAA
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/mscomhp/_scrf/js/themes=default/42-d5301b/a4-539297?ver=2.0
Preview:	require(["jqReady!"],function(n){function v(n,t,i){i.setAttribute(o,"false");p();n.contentWindow.postMessage({action:"open"},t);e||(e=document.getElementById(k));e.style.display="none";e.getAttribute(o).toLowerCase()==="false"&&e.setAttribute(o,"true")}function d(){if(t||(t=document.getElementById(u)),i||(i=t.getAttribute(f)),s||(s=document.getElementById(w)),s){var n=s.getAttribute("data-lpcurl");t.contentWindow.postMessage({lpcurl:n},i)}function y(n){t||(t=document.getElementById(u));i||(i=t.getAttribute(f));t.contentWindow.postMessage({invite:n},i)}function p(){t||(t=document.getElementById(u));i||(i=t.getAttribute(f));var n=t.getAttribute("data-chatTopic");l||(l=t.getAttribute("data-isOfficeCommercial").toLowerCase()==="true"?"Office365":n?n:"Store");t.contentWindow.postMessage({action:"parentsize",Width:window.innerWidth,Height:window.innerHeight},i);t.contentWindow.postMessage({action:"Topic",Topic:l},i)}function g(){if(t||(t=document.getElementById(u)),!t){var i=t.getAttribute(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\de-ch[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	178717
Entropy (8bit):	5.396381688030545
Encrypted:	false
SSDEEP:	1536:qHmIRHJ9Zm4nzKF5ZHKKh1LGYhz3jEj9TNfHx7EmI9oNwT7YadEeFX8BUjRhggXR:qlRrLU6YjT7YadEeFEOV
MD5:	D233CD5EA4B34251E09E151943651991
SHA1:	74237A119A3A5C5E52D740861DAAF276AF29F0FD
SHA-256:	ED00C1B58108F03BE9AC7524D433782AA39A877739A817C0B3177D8466AB3475
SHA-512:	667F2F7325F232A81B8C9325837F3231FA5E18575DE86A5B69F9BD5BB3DC60D8AABA57ABDA5CEDCF77A12C38F040612D5953A0B3756D313BC746E4A98A9C10A4
Malicious:	false
Preview:	......<!DOCTYPE html>..<html lang="de-ch" dir="ltr">..<head data-info="{"v":"1.0.7621.39544","a":"f4121db1-2de3-4ba3-b08e-be9366c5f4f0","cn":"OneDeployContainer","az":"{did:92e7dc58ca2143cfb2c818b047cc5cd1, rid: OneDeployContainer, sn: marketingsites-prod-odnortheurope, dt: 2018-05-03T20:14:23.4188992Z, bt: 2020-11-13T05:58:08.0000000Z}","ddpi":"1","dpio":"","dpi":"1","dg":"uplevel.web.pc.ie","th":"default","m":"de-ch","l":"de-ch","mu":"de-ch","rp":"/de-ch/","f":null,"bh":{}}">.. <meta charset="UTF-8" />.... <meta http-equiv="x-ua-compatible" content="ie=edge" />.. <meta name="viewport" content="width=device-width, initial-scale=1" />.. <title>Microsoft . Offizielle Homepage</title>.. ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\facebook[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	265
Entropy (8bit):	6.681697500155679
Encrypted:	false
SSDEEP:	6:6v/lhP1RnDsp9ULc5k6sc+7IhXxXA1MiyphxiDw66yVUjqIbp:6v/79GCc5kAhqMpph8UyWq6
MD5:	352637E02A377A29073AA9F65B1FBA22
SHA1:	E5E2B07F777F47DCF158120B11D0B6BDEB0BC878
SHA-256:	C77873C0C4A8499BA493832E950D41CBAEE43020D5C99D702A1E9DEBBAF0DB32
SHA-512:	DFDF4B94AC252B67E6D255C708505845AD427CEC4155D4C2796B84AC49658D6D140CC3744A5BA7A2F4F7AE989EC89D1F13271AAAC44ADF15D8553F45BBF447A
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/_h/85288795/coreui.statics/images/social/facebook.png
Preview:	.PNG.....IHDR... ... .tEXtSoftware.Adobe ImageReadyq.e<....IDATx.bt.].@K..@c0j.A.B....Vey.....T...X:>PKYN.Y.9n5u,...m..a.dG..6..C...].O.=..V....D.>8.)0z1.)D....@....H...(.....0.^..J.8x.....W.....-.G-..`0V.....8.....@2..M....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\jquery-3.3.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	86929
Entropy (8bit):	5.289492706499139
Encrypted:	false
SSDEEP:	1536:aLiBdiaWLOczCmZx6+VWuGzQNOzdn6x2RZd9SEnk9HB96c9Yo/NWLbVj3kC6ta:+kn6x2xe9NK6nC6E
MD5:	378087A64E1394FC51F300BB9C11878C
SHA1:	0C3192B500A4FD550E483CF77A49806A5872185B
SHA-256:	4FE68FA216176E6D1F4580E924BAFECC9F519984ECC06B1A840A08B0D88C95DE
SHA-512:	9A2C70516EA0C8C37C7F072F214DE0AFD5DDEB643C6B5D3FA8ADE3EF8D2CE40BDF8B1B1194BAD296E9075562701EE7DAE48B18144B1CD2D735328BE5A3ACBE6
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\jquery-3.3.1.min[1].js	
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/_h/46c44584/coreui.statics/externalscripts/jquery/jquery-3.3.1.min.js
Preview:	/*! jQuery v3.3.1 | (c) JS Foundation and other contributors | jquery.org/license */..!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery requires a window with a document");return t(e)}:t(e)}("undefined"!=typeof window?window:this,function(e,t){"use strict";var n=[],r=e.document,i=Object.getPrototypeOf,o=n.slice,a=n.concat,s=n.push,u=n.indexOf,l={},c=l.toString,f=l.hasOwnPropery,p=f.toString,d=p.call(Object),h={},g=function e(t){return"function"==typeof t&&"number"!=typeof t.nodeType},y=function e(t){return null!=t&&t===t.window},v={type:!0,src:!0,noModule:!0};function m(e,t,n){var i,o=(t=t||r).createElement("script");if(o.text=e,n)for(i in v)n[i]&&(o[i]=n[i]);t.head.appendChild(o).parentNode.removeChild(o)}function x(e){return null==e?e+"":"object"==typeof e||"function"==typeof e?l[c.call(e)]||"object":typeof e}var b="3.3.1",w=function(e,t){return new w.fn.init(e,t)}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\lp_ada_enhancements-prod[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	213113
Entropy (8bit):	4.773638065316456
Encrypted:	false
SSDEEP:	1536:S//9L5F4Y9T46deYJEamUZXG4Tsdfyr96dlw97Xmho8fhk8gpDhrpvUvTtkyOCrO:OuN7wzZYFbVuyArH7FMvS9Id/zm5jx9h
MD5:	4AE4E43473D56F9A563F0AB103E6D8F2
SHA1:	A5E3EB6723DBC3D42B37839AE97A12CA56F2B955
SHA-256:	FB42F86E1A73952BA7F37E316CD666364DD86CA1A6E7E7FA3B3D74B3EF0B37EA
SHA-512:	3D86F151CF7F3A787A8DAC5A0594A682F8E1E55ABE8BEBC291D45516F9AF84E9B619512C01136E4006B19869BE098BD61D031E9A56DDD5B0601C4B35CE1E1527
Malicious:	false
IE Cache URL:	http://https://static-assets.fs.liveperson.com/microsoft/lp_ada_enhancements-prod.js
Preview:	var engagementFix = (function() {. var engEl;.. function focus(eng) {. // Run if a button was detected. if (eng.engagementType === 5) {. // Look in dom for a role of button. We only need to do this once because each button load will cause this to run.. setTimeout(function() {. var button = document.querySelector('[role="button"]');.. if (button) {. button.removeAttribute('role');. }. }, 200);. }.. if (eng.engagementType === 23) {. document.querySelectorAll('[data-LP-event="close"]')[0].click();. }.. engEl = document.getElementById("chatEngagement"); .. if (engEl != null) {. setTimeout(function() {. document.getElementById("chatEngagement").focus();. }, 200);. } else {. setTimeout(function() {. var engagementContainer = document.getElementsByClassName('LPMcon

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\me[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	10273
Entropy (8bit):	5.436492601990225
Encrypted:	false
SSDEEP:	192:pDxv1n+7Xr+cHEzFQD6Ds35b05e58ITZSTXh7gk0yi4Bw9smd8:pVQ7XrUJds35bd8cAYdu
MD5:	965BD2EA836865484B6DEAE541284581
SHA1:	176061B4A0E0A7F4E6B8D484892A96C26914F4BA
SHA-256:	62AB1ADF3DF6E0D3484FD74E60B511F154685257FFFCB019A4EED74DF34FD58E
SHA-512:	5311C4D1710025F69AC03370C073BC39885F8F67BC6982E12B501AFF6DBE085FAF136ECEEB46292499B708FE1EA6226B4DA370B98A675DA1812B1CBC3CEAF6E4
Malicious:	false
Preview:	Copyright (C) Microsoft Corporation. All rights reserved. --><!DOCTYPE html> ServerInfo: BL02PF1A2651928 2020.10.23.21.27.05 Live1 Unknown LocVer:0 --> ProcessInfo: azbldrun:AzBuildW2-Ha13, 2020-11-23T03:56:21.9041428-08:00 - Version: 16,0,28799,16 --> RequestLCID: 1033, Market:EN-US, PrefCountry: US, LangLCID: 1033, LangISO: EN --><html dir="ltr" lang="EN-US"><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"/><base href="https://login.live.com/pp1600/"/><noscript><meta http-equiv="Refresh" content="0; URL=https://login.live.com/jsDisabled.srf?mkt=EN-US&lc=1033&uaid=c28eecea3263419e365f34270019379f"/>Microsoft account requires JavaScript to sign in. This web browser either does not support JavaScript, or scripts are being blocked. To find out whether your browser supports JavaScript, or to allow scripts, see the browser's online help.</noscript><title>Windows Live ID</title><meta name="robots" content="none" /><meta name="PageID" co

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\mwfmdl2-v3.54[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26288, version 0.0
Category:	downloaded
Size (bytes):	26288
Entropy (8bit):	7.984195877171481
Encrypted:	false
SSDEEP:	768:56JqQaQphRbTHiKNF5z/02h5KpJW3pPOA8Y9g/:gdTTH5XKpJWdH1W/
MD5:	D0263DC03BE4C393A90BDA733C57D6DB
SHA1:	8A032B6DEAB53A33234C735133B48518F8643B92
SHA-256:	22B4DF5C33045B645CAFA45B04685F4752E471A2E933BFF5BF14324D87DEEE12
SHA-512:	9511BEF269AE0797ADDF4CD6F2FEC4AD0C4A4E06B3E5BF6138C7678A203022AC4818C7D446D154594504C947DA3061030E82472D2708149C0709B1A070FDD0E
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/mwf/_h/v3.54/mwf.app/fonts/mwfmdl2-v3.54.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\mwfmdl2-v3.54[1].woff	
Preview:	wOFF.....f.....D.....OS/2...X...H...`JM.FVDMX.....^.qcmap.....*.9cvt ...4... ...*....fpgm...T.....Y...gasp...D.....glyf...P..U5.....head..]....2...6.. .Chhea..]....$$...hmtx..]....ye'loca..^.....Gmaxp..`.... ... ./..name..`....8....]..Rpost..f..... .Q.wprep..f$.....x...x.c`.Pf.....:....Q.B3_dHc..`e.bdb... .`@..`...../9.|... V...)00...-.Wx...S....._..m.m.m.m.m;e..y.~.....<p..a.0t.&...a.pa.0B.1..F...Q.ha.0F.3....q.xa.0A.0L.&...l.da.0E.2L....i.ta.0C.1..f...Y.la.0G.3.....y.|a..@X0,....E.ba.DX2,....e .ra..BX1..V...U.ja..FX3.....u.za..A.0l.6...M.fa.E.2l....m.va..C.1..v...].na..G.3.....}.~a.p@80.....C.a..pD82.....c.q..pB81..N...S.i..pF83.....s.y..pA.0\....K.e..pE.2\....k.u..pC.1..n...[. m..pG.3.....{.}...@x0<.....G.c...Dx2<....g.s...Bx1..^...W.k...Fx3.....w.{...A.0|.>...O.g...E.2|....o.w...C.1..~..._.o..08.....?..0$.....x...mL.U.....9.x.`[...&BF@X...V.h.Z..h. .....`n....[..U

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\social[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	405050
Entropy (8bit):	5.009061808550039
Encrypted:	false
SSDEEP:	3072:GAwmeEZACGwzyP5kTP3bI0tfYqQ0xtLfj4ZDa813giY8R1j35Ap7zzN1n1JKfNkW:CEZACgj
MD5:	12388E77823064F20C2AC22E7BD5A6CB
SHA1:	9E000D34F5140CB3B2B6AE471C7B7FA6CDD11520
SHA-256:	78E235423A915B16AF695D8B0D6EF7F994779EC33DC4452C79DB7A48DCE45FAB
SHA-512:	F248B25390386DABC541EF85383204875C2AFAF21DE3A466A9710F076FEB6B7BB0E1EA26161FFB803C8056DA03C90C85676963AB197A35CC20F789029ED41323
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/mwf/css/MWF_20201028_28422223/west-european/default/alert/autosuggest/contentplacement/contentplacementitem/flipper/flyout/glyph/heading/hero/heroitem/hyperlinkgroup/image/list/pagebehaviors/singleslidecarousel/skiptomain/social?apiVersion=1.0&include_base=true
Preview:	@charset "UTF-8";./*! 1.57.0 | Copyright 2017 Microsoft Corporation | This software is based on or incorporates material from the files listed below (collectively, "Third Party Code"). Microsoft is not the original author of the Third Party Code. The original copyright notice and the license under which Microsoft received Third Party Code are set forth below together with the full text of such license. Such notices and license are provided solely for your information. Microsoft, not the third party, licenses this Third Party Code to you under the terms in which you received the Microsoft software or the services, unless Microsoft clearly states that such Microsoft terms do NOT apply for a particular Third Party Code. Unless applicable law gives you more rights, Microsoft reserves all other rights not expressly granted under such agreement(s), whether by implication, estoppel or otherwise.*/./*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */.html{font-family:sa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\tag[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):	21652
Entropy (8bit):	5.471454971272349
Encrypted:	false
SSDEEP:	192:speXIcO8AiGMXMGc1IajSFkhChE7KYHliXMvjmPc3l7jcCVVmF6Q+3vMjT8LEc6q:sp63F4M3jFkfHlHL91cCVVbO8IkFAjl8
MD5:	E2EE8A9CD68C3D310A4C62FDB4B5C93A
SHA1:	67EB5F9547F1D9DE0A8B143C3B50511C26281399
SHA-256:	145D14BB73E5B03CC73062C2A78C392125B891C62B1CC9D542E5ADBA762F04E7
SHA-512:	4CFEE56CA068134354BE94127465E9AA7BFD8F68E0D2B6D6A367C0E9EACA5CDF5FC39290F6C1CB3DD4DC9319B60A38F810F220AD836C94FEDC991AE17EB8259
Malicious:	false
IE Cache URL:	http://https://lptag.liveperson.net/tag/tag.js?site=60270350
Preview:	window.lpTag=window.lpTag||{};lpTag.taglets=lpTag.taglets||{};lpTag._tagv="4.1.2";!function(a,b){function c(c,d,e){b._logcnt=b._logcnt||0;H(c,d,e,b._logcnt);if("undefined"!=typeof a.lpTaglogListeners&&a.lpTaglogListeners.constructor===Array)for(var f=0;f<lpTaglogListeners.length;f++)try{lpTaglogListeners[f](c,d,e,b._logcnt)}catch(g){H("Exception="+g.message+" msg="+c,d,e,b._logcnt)}b._logcnt++}function d(a){if(a)for(var b=0;b<a.length;b++)qa[a[b].service]=a[b].baseURI}function e(){for(var a=Ga.PRODUCTION,c=b.ovr&&b.ovr.domain,d=0;d<Ha.length;d++)if(Ha[d].tagDomain===c){a=Ha[d].env;break}return a}function f(a){var b;a=a||e();if("string"==typeof a)for(var c=0;c<Ha.length;c++)if(Ha[c].env===a){b=Ha[c].tagDomain;break}return b}function g(a){var b=qa[a],c="ALL";return b?b:qa[c]}function h(){return qa}function i(a){return l(ra,a)}function j(a){return l(sa,a)}function k(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])}function l(a,b){var c;c="undefined"!=typeof b?"undefined"!=typeof a[b]?

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\RE3Vc2M[1].wdp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG-XR
Category:	downloaded
Size (bytes):	11254
Entropy (8bit):	7.880173884953612
Encrypted:	false
SSDEEP:	192:5Q6BZuMcEXd96jvzn14khb5mCqAnOlWj/8vtqyGUgNu7+VQch:dcasjbb0eOw1lYNy+V
MD5:	2F14EC6C098C98BE1D02125E26C446B6
SHA1:	CB835BDC771A61C3E45EAEE0A51C9FB7C27563BF
SHA-256:	B11B3885B20ED463D1F04957E29A4D24F82E805C16F53623E8822A870B84DDE8
SHA-512:	599C189728E35812BD50306110A2ADF03C163E4D3A57E0EDCE1B0CC03EBA752A96215C527C4E6C9BD534B2D606F3667A78458F575DA55D8FBB902FAC5719636
Malicious:	false
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE3Vc2M?ver=4043&q=90&m=6&h=201&w=358&b=%23FFFFFFFF&l=f&o=t&aim=true

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\RE3Vc2M[1].wdp	
Preview:	II.. ...$..o.N.K..=wv.....f.....$..B.....$..B.....p+.....WMPHOTO..E.q.e..0...,8:B.. ...../.]'K.....0,...E....$8.....i.h..a..?..o...."@2....iL .45...R'..P,.6.....2_..}.Iu.>.....V....m..$.(.`..u..R.6..I}*LI....D...K.g:3.I..KWW.=0....e.4...N..x\....]..B..''..kt...Qrr.-vO..]04>.v.K....D..".b./....e.U...n.STX)...I$0:.I.....$]..*.4y.J\...R...kb. h..g..T%{f....V.A`.,...H.R./$].P.uf..ba.n3p K.V..^...5p..4{;....."{h..n<M....N..a.....zSTI.....f..%.SU.J.1GY8... ....A..ZG.(!#V...!..D....!.zt.Q.A...T<..'.%...U4$...-<....p$.....I.....!. ...P.%Y,U.b..3wt..T...J.....DU.\f[..D..6^!.....sY..D...z.Y,..z..H..cF.....Hv.Rv.-.S.Hb.C...S.....P-,.....`.1.....K$.1%....A.....(....`.D7...w..'..}...1Da..4b....H._..Xp.....`.Kd.....h.G.6... c.....j.....J.)..j.7<\..|.....y&.P..vx.-...8..1..]H=.k..eW.....M.....1.....".%J.....I.@.)_.%8.....a..C0".R..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\RE4rriw[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 40 x 40, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	546
Entropy (8bit):	6.67436138738567
Encrypted:	false
SSDEEP:	12:6v/7cIaddcY0rdwfbgihih12ovMSvA1jsKi3Xr+gijQ5Wk7R:rIadeHrdAbghr2p49+gEQ5WkF
MD5:	303D29F63674D6C75DE78CCE52660968
SHA1:	37753DAA92E464CE71C6EBA767B77DA227600C2C
SHA-256:	0850AA4CB7CF87C5059C0F503CFED9DABEDECF303C62B3827B70C63B82FA54AA
SHA-512:	264FFD8FE525CC96B9DB58CEFEBB6836C2A1B38EF9736C29844CDF3E10A5BAB282A13CCCC9C16D2DE9BA2EB25F1338315DA1CA95BEC6939425344BE8A4402 CB1
Malicious:	false
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4rriw?ver=b2d5&q=90&m=6&h=40&w=40&b=%23FFFFFFFF&l=f&o=t&aim=true
Preview:	.PNG.....IHDR...(...(..... H_....PLTE.....*....1tRNS.r.....0a`:h.....@..P... <.;..>..+ .!..b(...V.....orNT..w.....sRGB.....IDAT8.....0....;FQP..*...?gl$.%da..V..]0.9!.....Kw.R.%)..TXAU.UT4.&.....E.....lY.h.g.67H.....:.2..>..N.s...<.:\ B.ok.`v.w.G...3 cn.....Oaj.....u.....}..5.1...h!.....z9.3.....;....f.....+T...s.....~.3.;...cf.....;..;4.Un.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\cartcount[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1283
Entropy (8bit):	4.393500974386876
Encrypted:	false
SSDEEP:	12:KPgkrfXKLf7fcabNBGFMpYMNwy+Mz4zMGgZv4c0EgtiQ5FgWyb0gDIgdcZPx+Ydg:KPv6HUY5+yAZFAXJqiXZXTMK
MD5:	1BF3F6D72753254D68A4A8C99DB850AD
SHA1:	E98B92CFF496817E3D5E6CD117F06BEEFAAD3E5F
SHA-256:	68D929A10C3CD609B936B50A541533994B044B38558A33530FF45D1B420CC07E
SHA-512:	C2F17E5861E800E32F3AC3DEA7424384E82B2F27B79C14D24686C286D5A6559CABDABB6A58DF9125334E196CC7D3116B583B3AE1D9AE6711AB21F9F4B06AF2C 0
Malicious:	false
Preview:	.....<!DOCTYPE html>..<html>..<head>.. <title>title</title>..</head>..<body>.. <script>.. function getCartItemCountFromCookie() {.. var name = 'c artItemCount=';.. var allCookies = document.cookie.split(';');.. for (var i = 0; i < allCookies.length; i++) {.. var c = allCookies[i];.. while (c.charAt(0) === ' ') {.. c = c.substring(1);.. }.. if (c.indexOf(name) === 0) {.. return c.substring(name.length, c.length);.. }.. }.. return 0;.. }.... var count = getCartItemCountFromCookie();.... var parentHost = '';.. var parentOriginProtocol = '';.. var pare ntOrigin = '';.. try {.. parentHost = parent.location.hostname || '';.. parentOriginProtocol = parent.location.protocol;.. parentOrigin = parent.locat ion.origin;.. } catch {..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\e3-082b89[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):	111882
Entropy (8bit):	5.228428046636105
Encrypted:	false
SSDEEP:	1536:uzUHQcyAz9ppxS7grUU59gQ9lwInL2dS6J09RhY8WOyd1EwgXA9GKaWAMKihAGD2:uzUnppxvIeJ0y9d1EwgXA9JKinDCE54
MD5:	FAD5CCD0C635DDA1F1AACE4F40E82BDC
SHA1:	8571197DA53E3328BF54DBF2226CDF62CF16DB4F
SHA-256:	950A8DC0EC6C07598BE52251F3C0FF655B61AC4003794A686BCBA5AFB0A1E09B
SHA-512:	D13336475554B7B6106B505E1D0190C0565C3E5259C7C800D143CA7DB08871ACCD19CFC120310571CE0DCA22BF4BFCFAE46CF9F25B98AF5F4DAFA87D975EC6 4
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/mscomhp/_scrf/js/themes=default/2f-63ce8f/45-f9a0d4/aa-dc1460/2d-7a9063/dc-7e9864/4f-5115f8/7d-266f10/4a-abd94b/6d-c07ea1/29-1ec5a9/23-c64e70/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/f8-73a5f2/79-499886/7e-cda2d3/b2-7087f0/e5-08f1c0/91-97a04f/1f-100dea/33-abe4df/50-f1e180/e3-082b89?ver=2.0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\e3-082b89[1].js	
Preview:	var __extends;define("ajaxWithAnimation",["jqReady!","jsll"],function(n,t){var i=[" <\/span><\/span><\/span><\/span><\/span><\/div>"],u=function(t,r){var u=n(t),o,f,e;u.length&&(o=(r.loaderType||"").toUpperCase(),i[1]=o==="PROGRESS"||o==="PROGRESSBAR"?"regional":o==="SPINNERLARGE"?"local f-progress-large f-center":"local f-progress-small",r.margin&&r.margin.length&&(i[3]=r.margin),f=i.join(""),e=(r.loaderPosition||"").toUpperCase(),e==="TOP"||e==="BOTTOM"?(u.addClass("ajaxloader"),e==="BOTTOM"?u.append(f):u.prepend(f)):(u.parent().addClass("ajaxloader"),e==="BEFORE"?u.before(f):u.after(f)))},f=function(t,i){var r=n(t),u;r.length&&(u=(i.loaderPosition||"").toUpperCase(),u!=="TOP"&&u!=="BOTTOM"&&(r=r.parent()),r.removeClass("ajaxloader").children().remove(".c-progress"))},r=function(i){i.refreshElement&&u(i.refreshElement,i);var r=n.extend(i,{s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the website you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\iframe[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	44323
Entropy (8bit):	5.156344556405993
Encrypted:	false
SSDEEP:	384:s5C3pnw64Mhe7R0TPjREHVrlwyzSFu2InWSCr1p1Xo:hP4OgR0fR2VriyWg1Wz1p1Xo
MD5:	8E57F3E827AECD5F5C542AD101D3D07E
SHA1:	4840156689DFDAF359C3F8A4B8D43E5A52058247
SHA-256:	5CA99E4C8BCB89C69950A8FE1DBCAC4E533E24A3AE865A2F07CF5931B2EA82D8
SHA-512:	98235CB56EB6FCD6DBA9178A73B3AC1F50E25DC4D55CC09D8F334F26DD846E5F04E10CB471AC41CEE7FEC70104E01D1AC520691474F164FAB675BF07037AA3CC
Malicious:	false
Preview:	<!DOCTYPE html>.<html lang='en'>.<head>..<title>iFrame Cart Page</title>..<meta charset='utf-8'>..<meta http-equiv='X-UA-Compatible' content='IE=edge,chrome=1'>..<meta name="format-detection" content="telephone=no"/>....<meta name='viewport' content='width=device-width,initial-scale=1.0,minimum-scale=1.0, maximum-scale=1.0, user-scalable=no'/>...<style>...body {....background-image:url('https://lpcdn.lpsnmedia.net/le_unified_window/9.12.0.19-release_4769/resources/loader_on_warmGray5_75.gif');....background-repeat: no-repeat;....background-attachment: fixed;....background-position: center;...}....@font-face {....font-family: "Segoe UI";....src: url("https://c.s-microsoft.com/static/fonts/segoe-ui/west-european/normal/latest.woff2") format('woff');...}.....* {....font-family: "Segoe UI", Arial, sans-serif !important;...}....body #lpChat .lp_dialog_container .lp_buttons_area .lp_confirm_button {....color: #000 !important;...}.....lp-iframe-window, .lp_desktop #lpChat > .lp_maximized {..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\jsll-4[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):	56283
Entropy (8bit):	5.402458596770319
Encrypted:	false
SSDEEP:	768:0tgoOjNcc6rCDBjPSeAaKU7rD8kcK7hAHZcllEiKjkT3dgD4GD1hrTd8PuWCF9IS:0tV81ICDVRQihAiUinxgDRQ7wYv6p
MD5:	AD8545B54A7D77B1EF0E02AFB615A107
SHA1:	3E1BE466B952F8A07E04D6187A90C4A7F9D15D28
SHA-256:	196D3E71A396F75F52B94BF617E5F4474B85CA2F358F32CC81D3521731FDE20C
SHA-512:	62E938CF070F47F475E2088C32E6DC12E2D9F6ED40E25920E52B5CC6C973947684BFFC1B1371C4D79E84C005A86E98A2119A0888FB784FD7B76F8DA413576BE5
Malicious:	false
IE Cache URL:	http://https://az725175.vo.msecnd.net/scripts/jsll-4.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\jsll-4[1].js	
Preview:	var awa=awa||{},behaviorKey;awa.isInitialized=!1;awa.verbosityLevels={NONE:0,ERROR:1,WARNING:2,INFORMATION:3};awa.behavior={UNDEFINED:0,NAVIGATIONBACK:1,NAVIGATION:2,NAVIGATIONFORWARD:3,APPLY:4,REMOVE:5,SORT:6,EXPAND:7,REDUCE:8,CONTEXTMENU:9,TAB:10,COPY:11,EXPERIMENTATION:12,PRINT:13,SHOW:14,HIDE:15,MAXIMIZE:16,MINIMIZE:17,BACKBUTTON:18,STARTPROCESS:20,PROCESSCHECKPOINT:21,COMPLETEPROCESS:22,SCENARIOCANCEL:23,DOWNLOADCOMMIT:40,DOWNLOAD:41,SEARCHAUTOCOMPLETE:60,SEARCH:61,SEARCHINITIATE:62,TEXTBOXINPUT:63,PURCHASE:80,ADDTOCART:81,VIEWCART:82,ADDWISHLIST:83,FINDSTORE:84,CHECKOUT:85,REMOVEFROMCART:86,PURCHASECOMPLETE:87,VIEWCHECKOUTPAGE:88,VIEWCARTPAGE:89,VIEWPDP:90,UPDATEITEMQUANTITY:91,INTENTTOBUY:92,PUSHTOINSTALL:93,SIGNIN:100,SIGNOUT:101,SOCIALSHARE:120,SOCIALLIKE:121,SOCIALREPLY:122,CALL:123,EMAIL:124,COMMUNITY:125,SOCIALFOLLOW:126,VOTE:140,SURVEYINITIATE:141,SURVEYCOMPLETE:142,REPORTAPPLICATION:143,REPORTREVIEW:144,SURVEYCHECKPOINT:145,CONTACT:160,REGISTRATIONINITIATE:161,REGISTRATIO

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\latest[1].woff2	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format (Version 2), TrueType, length 34052, version 0.0
Category:	downloaded
Size (bytes):	34052
Entropy (8bit):	**7.994131533337155**
Encrypted:	**true**
SSDEEP:	768:WHH8jjaseVFXnmQ8njOkV5c4d7DOgx1J89JzHNBbFOlsy0kQ6lhe:kH8jj3uWxKe5c4xz69hNalP0kQ6lhe
MD5:	36397A3BC139C6E9F81D383F060F080A
SHA1:	3F4F86C10920D4ED345F4858B6CDE9F93E1AEB81
SHA-256:	4F7F4AFE26E71FA9CA1DAC4A43B557A554A46F53251D849F07ED08A04829D74B
SHA-512:	7FFF4870E9142E6E1921F8DD78E3B049547EC1D540EFE573C2938F8B855DB61BA908FA9D3C8DA1BB2AAE6D95217A586D256B9EA2BD8A8F706B1DB75BC21F2CB9
Malicious:	false
IE Cache URL:	http://https://c.s-microsoft.com/static/fonts/segoe-ui/west-european/normal/latest.woff2
Preview:	wOF2.....`....."..\.....D..D.6.$..... .. . ..@.S.5x.q..m.5.7Q..2.....6..R....v.j....."..c..@.Z.B..G.Y.\S.AtT.iTJt....l.>..=+z...1.pP..[.+.S..`...c.1.u1...).....`.. .....9.8.....+..4...;..[W.v..p0..qg..=..+...1...|R..qM..|/...%..!C.....G:.;7...Z..^P...o..q.B'....a....M.l3k....=&.'.'..8.....K..k.....}.?w.i[..q.,...,0,.....?...o.y..@..U5.:T..E..B..%..... .YU.....Z..4T..5....m/..,$.w..`O.s.c.{...;a;..T...9../.....,....BDf.S).ola._e../..z%.:....r..d;.t....7....jl!-.....{..l.T..H%8.p.**=!.z8.7.k..L...WUW...0.0.....7Q.0.J..Q.|~P..'Q... m.a..(..p..q.*. .B.:.....e.B...g..<O(..z..o.G...U.x.Tw...^t._..t..}....q....*K....".UP...Te...<.....f.....{.....l..V...p.+...-<..%.+..?M.A!.ob.9p...7..B. ..R....."4..%M.6..'...!.S.....?.`w.....l@..R.AJ&@..h/H{. (n..I.8..6.4 ..i{..5.I....l...rJ.....N{.^..6..^.V.&..)?Bc.&.u.....fd.H..X.5Fq(c....6...w(O..K...F.....ohh.....Gk...l.2q.t.h.....U9%.n....%...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\linkedin[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	340
Entropy (8bit):	6.89748464898483
Encrypted:	false
SSDEEP:	6:6v/lhP1RnDspTAkgcqadiGjXMnThBRqDOLWlQ78GwKjFkYCaprI51Fu/Vp:6v/79G9AIqa4GrMnFql+7xjFmirIoz
MD5:	082196E344000587C008B768820283B6
SHA1:	A0A3A982764456CF74F75B47F7B5C517A628E586
SHA-256:	A91DC0F2545A1929E0C6A180C1728C433B23602A4C8AEC06552F5604525689CA
SHA-512:	FDBC29F6D3DF628007683DD6D8A8F3F0FA1CF743C72AC1F078F2C5FE37A360182B1CBA371F0F20B4F795F3BC3A1135103A2BCE190F69FA7ED8E31205CEF6C9A
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/_h/b23f9ba2/coreui.statics/images/social/linkedin.png
Preview:	.PNG.....IHDR... ... .tEXtSoftware.Adobe ImageReadyq.e<....IDATx.bd,..@K..@c0j..[..).o,..).....g/<.De.@L.2..9..Q?. .C..$..-.....K.[....p?x.]..K.Z.H..<m.....L.@. ...7^}Y...../D.Vl.....`.:.:.i.9...tHz.V.mN.....@.....3.9.L<.`..'...../..g?D.T....oX.T..;V.h.6R-`.m.Z@1..0..Ec^..|.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\twitter[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	532
Entropy (8bit):	7.480175935964278
Encrypted:	false
SSDEEP:	12:6v/79GsdpT04EoI/TGxLd1sjDBdqktOeUoOzQag23jEAgc:SdpfdUyxpgMb1zpg2Tpp
MD5:	B30436EB503A7EA8E77925F435DF4671
SHA1:	3313C5FDE8EC85B94547168B867EFEC0188F5987
SHA-256:	0AC4630B76827B89EBEA070A1BEB6E5175D280EADC76B67FA886CF6068368CA3
SHA-512:	CE6B7F9D8860E146CD41802FBD30AE99F205D145CCA4BBECBAB446851165BEE8316FEAABD83826FB31CA97652E911BE4815ED542F33B5BFEAABDCF71BCEFCDC8
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/_h/93690392/coreui.statics/images/social/twitter.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\twitter[1].png	
Preview:	.PNG.....IHDR... ... .tEXtSoftware.Adobe ImageReadyq.e<....IDATx..V=O.P.....u`.A.q...eU.....YW..q.UYHD.M.A.]:Xc4..X<.1....&..Ci.;..s.T./?bQF".q....@..G.O. .r^....q.j...4F.C.....ik.....".....r>.V..^}.H.u....g2...\t7....p.5.C...?..8.....IW...j.x._Ay-S)....bi...B..c.Yk@.....$.....$.@.F....X...B#...*9U.y.to%.m.u.2....Kp.;....b....N..@y..MkL.Fg.-%.~.....Cq.#W4J0.xP..R.+1..kdPm.kw...n.+B..d..J!.p....5..T..84..$..3..O5...m.SHmz..\.ULX._.q....r...f.....h8..g.4...0..\|.o$..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\wcp-consent[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):	255440
Entropy (8bit):	6.051861579501256
Encrypted:	false
SSDEEP:	6144:PIgagvUI0iDsW9Whsredo7NjIZjIZP0aNWgF9Dyjzh:PIgaHI0iIUedo7NjIZjIZP0o74t
MD5:	38B769522DD0E4C2998C9034A54E174E
SHA1:	D95EF070878D50342B045DCF9ABD3FF4CCA0AAF3
SHA-256:	208EDBED32B2ADAC9446DF83CAA4A093A261492BA6B8B3BCFE6A75EFB8B70294
SHA-512:	F0A10A4C1CA4BAC8A2DBD41F80BBE1F83D767A4D289B149E1A7B6E7F4DBA41236C5FF244350B04E2EF485FDF6EB774B9565A858331389CA3CB474172465EB3F
Malicious:	false
IE Cache URL:	http://https://wcpstatic.microsoft.com/mscc/lib/v2/wcp-consent.js
Preview:	var WcpConsent=function(e){var a={};function i(n){if(a[n])return a[n].exports;var o=a[n]={i:n,l:!1,exports:{}};return e[n].call(o.exports,o,o.exports,i),o.l=!0,o.exports}return i.m =e,i.c=a,i.d=function(e,a,n){i.o(e,a)||Object.defineProperty(e,a,{enumerable:!0,get:n})},i.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object. defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},i.t=function(e,a){if(1&a&&(e=i(e)),8&a)return e;if(4&a&& "object"==typeof e&&e&&e.__esModule)return e;var n=Object.create(null);if(i.r(n),Object.defineProperty(n,"default",{enumerable:!0,value:e}),2&a&&"string"!=typeof e)for(va r o in e)i.d(n,o,function(a){return e[a]}.bind(null,o));return n},i.n=function(e){var a=e&&e.__esModule?function(){return e.default}:function(){return e};return i.d(a,"a",a),a},i.o =function(e,a){return Object.prototype.hasOwnProperty.call(e,a)},i.p="",i(i.s=1)}([function(e,a,i){window,e.exports=function(e){var a={};function i(n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\zones[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):	18451
Entropy (8bit):	4.929550848681014
Encrypted:	false
SSDEEP:	192:GdjjSUaTGkgh1BvhEun6tuckPpE+ziELZZEyGRjZMIKJ56oDwPcQN9CAzy/qNcVV:k5fP/5ozV8R
MD5:	B718B8D27C0C9EF5E1E1CF35F754B01F
SHA1:	0F2A03DD931DD6DF4952F7DF2AB1E8C9113B87F1
SHA-256:	1CE2B747071605A71E62F65708B5B26BC5C370270F4AFF600D205B292EAD0D39
SHA-512:	8553184BA04A0D7744C670FAC96A58C2F14A7A29BA30DD0469B82575D15BA106435051E95A27007057C2BB7706E6173206F7815582A8FBEB6B1BAFF9D865CFFE
Malicious:	false
IE Cache URL:	http://https://accdn.lpsnmedia.net/api/account/60270350/configuration/le-campaigns/zones?fields=id&fields=zoneValue&cb=lpZonesStaticCB
Preview:	lpZonesStaticCB([{"id":138781714,"createdDate":"2017-02-28 18:44:28","modifiedDate":"2017-02-28 18:44:28","name":"Right Overlay","deleted":false,"zoneType":1,"m ainZone":false,"capping":0,"mapping":[{"engagementSubType":26},{"engagementSubType":17},{"engagementSubType":22},{"engagementSubType":19},{"engagement SubType":27},{"engagementSubType":24},{"engagementSubType":18}],"isDeleted":false},{"id":138781814,"createdDate":"2017-02-28 18:44:28","modifiedDate":"2017-02-2 8 18:44:28","name":"Offsite","deleted":false,"zoneType":2,"mainZone":false,"capping":0,"mapping":[{"engagementSubType":28},{"engagementSubType":29},{"engagement SubType":30}],"isDeleted":false},{"id":138781914,"createdDate":"2017-02-28 18:44:28","modifiedDate":"2017-02-28 18:44:28","name":"Left Overlay","deleted":false, "zoneType":1,"mainZone":false,"capping":0,"mapping":[{"engagementSubType":15},{"engagementSubType":25},{"engagementSubType":20},{"engagementSubType":21}, {"engagementSubType":14},{"engagementSubType":23},{"engag

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\65-478888[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	97410
Entropy (8bit):	5.072039972077101
Encrypted:	false
SSDEEP:	1536:Q2zddgKHPbn/hLOfbv3DlFeEqyf5Y6FtgAJL55OGHlkzmnez1ZIuUbMFmiRjJYJH:Q2zddgKHPbn/hLOfbv3DlFeEqyf5Y6F/
MD5:	8214332B4ED28AC7FAE2B53EF783EBCC
SHA1:	6E4B376F5FB9AE7D09CABCCE33CEB489CA5AFE52
SHA-256:	F67BF6642592F34371E1EDAFB9A4B3435BF57405DF0B593CE580E8138EE51598
SHA-512:	C0D2FD51E008ED02DAE3479D58CA4F7A299B1AFE3D1EF88772CC0473067290388B03C6DFDD9BDAE697ECD324752730782F9B2A6ED523608BE781EAB6DBBACF0
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/west-european/mscomhp/_scrf/css/themes=default.device=uplevel_web_pc_ie/a4-817070/71-66493b/37-e29aca/21-7d6c87/5a-e79275/16-a6d48e/65-478888?ver=2.0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\65-478888[1].css	
Preview:	..x-hidden-none-mobile-vp{display:none !important}@media screen and (-ms-high-contrast: active){.c-uhfh button,.c-uhfh .glyph-shopping-cart,.c-me .msame_Header{ border:none !important}.c-logo{margin-right:1px;border:none !important;outline:none !important}.c-logo.c-cat-logo:focus>span:before,.c-logo.c-cat-logo:hover>spa n:before{background:WindowText}.c-uhf-nav-link{border:none !important}.c-uhf-nav-link:hover{text-decoration:underline !important}#search{background:Window;color :WindowText}#search span{vertical-align:top}.c-uhfh.c-sgl-stck .c-uhf-menu button:focus,.c-uhfh.c-sgl-stck .c-uhf-menu a:focus,.c-uhfh.c-sgl-stck .c-uhf-nav-link:focus,.c-uhfh.c-sgl-stck .c-logo.c-sgl-stk-uhfLogo:focus,.c-uhfh.c-sgl-stck .c-logo.c-cat-logo:focus,.c-uhfh.c-sgl-stck .c-search #search:focus,.c-uhfh.c-sgl-stck .glyph-shopping-cart:focus,.c-uhfh.c-sgl-stck .glyph-global-nav-button:focus,.c-uhfh.c-sgl-stck .glyph-shopping-bag:focus{outline:2px solid WindowText !important}.c-uhfh.c-sgl-stck .c-uhfh-acti

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\94-3cd1e0[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):	68375
Entropy (8bit):	5.370837839922446
Encrypted:	false
SSDEEP:	1536:gtV81ICDVRgJhAiUinqgDRQ7wYv6uxhBANIu:gv81+einqgD8Q
MD5:	53475B50CF354A3E5CCBB0740A2AE553
SHA1:	9166969D9B0D89321B6BD0A754E3DEE54C2B7B11
SHA-256:	EEA90E1F236FD6CED5D08C19B424BC7D36A1679C3B87B71C560365AED4888FF3
SHA-512:	D53A98168F82CFDCC02CEF55D73EE40D4F1D32EDB8AC85256182D88F3609FEEAB7A5186B4527BC7B5AA77CB06930E324C8A56CB49F3CC71E1A02D5B5394396 7
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/mscomhp/_scrf/js/themes=default/78-6f121b/94-3cd1e0?ver=2.0
Preview:	var awa,behaviorKey;define("jsllConfig",["rawJsllConfig"],function(n){return n});awa=awa||{};awa.isInitialized=!1;awa.verbosityLevels={NONE:0,ERROR:1,WARNING:2, INFORMATION:3};awa.behavior={UNDEFINED:0,NAVIGATIONBACK:1,NAVIGATION:2,NAVIGATIONFORWARD:3,APPLY:4,REMOVE:5,SORT:6,EXPAND:7,REDUCE :8,CONTEXTMENU:9,TAB:10,COPY:11,EXPERIMENTATION:12,PRINT:13,SHOW:14,HIDE:15,MAXIMIZE:16,MINIMIZE:17,BACKBUTTON:18,STARTPROCESS:20, PROCESSCHECKPOINT:21,COMPLETEPROCESS:22,SCENARIOCANCEL:23,DOWNLOADCOMMIT:40,DOWNLOAD:41,SEARCHAUTOCOMPLETE:60,SEARCH:61, SEARCHINITIATE:62,TEXTBOXINPUT:63,PURCHASE:80,ADDTOCART:81,VIEWCART:82,ADDWISHLIST:83,FINDSTORE:84,CHECKOUT:85,REMOVEFRO MCART:86,PURCHASECOMPLETE:87,VIEWCHECKOUTPAGE:88,VIEWCARTPAGE:89,VIEWPDP:90,UPDATEITEMQUANTITY:91,INTENTTOBUY:92,PUSHTOI NSTALL:93,SIGNIN:100,SIGNOUT:101,SOCIALSHARE:120,SOCIALLIKE:121,SOCIALREPLY:122,CALL:123,EMAIL:124,COMMUNITY:125,SOCIALFOLLOW:126, VOTE:140,SURVEYINITIATE:141,SURVEYCOMPLETE:142,REPORTAPPLICATION:143,REPORTREVIEW:144,SURV

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\RE1Mu3b[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 216 x 46, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4054
Entropy (8bit):	7.797012573497454
Encrypted:	false
SSDEEP:	48:zICvnyRHJ3BRZPcSPQ72N2xoiR4fTJX/rj4sFNMkk5/p1k2lPUmbm39o4aL7V9XH:10nvE724xoiRQJPrjpLKSFl9oX31Z1d
MD5:	9F14C20150A003D7CE4DE57C298F0FBA
SHA1:	DAA53CF17CC45878A1B153F3C3BF47DC9669D78F
SHA-256:	112FEC798B78AA02E102A724B5CB1990C0F909BC1D8B7B1FA256EAB41BBC0960
SHA-512:	D4F6E49C854E15FE48D6A1F1A03FDA93218AB8FCDB2C443668E7DF478830831ACC2B41DAEFC25ED38FCC8D96C4401377374FED35C36A5017A11E63C8DAE5C 87
Malicious:	false
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE1Mu3b?ver=5c31
Preview:	.PNG.....IHDR.....J.....tEXtSoftware.Adobe ImageReadyq.e<...(iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpme ta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c132 79.159284, 2016/04/19-13:13:40 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http ://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:A00BC639840A11E68CBEB97C2156C7FD" xmpMM:InstanceID="xmp.iid:A00BC638840A11E68C BEB97C2156C7FD" xmp:CreatorTool="Adobe Photoshop CC 2015.5 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:A2C931A470A111E6AEDFA145 78553B7B" stRef:documentID="xmp.did:A2C931A570A111E6AEDFA14578553B7B"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.....DIDATx..\ ..UU.>.7..3....h.L..& j2...h.@..".....`U.....R"..Dq.&.BJR 1.4`$.200...l.....wg.y.[k/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\RE4CFyx[1].wdp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG-XR
Category:	downloaded
Size (bytes):	14392
Entropy (8bit):	7.87814533363795
Encrypted:	false
SSDEEP:	384:UULXeb+ZeNCvZWabSXcxTxa07i74vjvfcI:xeb+G8ZWa8cCEi7Ebf3
MD5:	0242F12621C4D5B412090CD05F235129
SHA1:	058A3D403331106E57E92BCE67BB40712635F80F
SHA-256:	29711D4EA2A8AE8F4F0931666107E06ADA6ABD6D87AA12788DCF34D69552E35B
SHA-512:	76589DBE4300F7C8D890AD2920B78B39B624CAF2CF310DC7395C85A1458176E45490FCBA4FFC9155F85601C64D362A1DB18DE8791E6C085E390E932BDF85166
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\RE4CFyx[1].wdp	
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4CFyx?ver=25c5&q=90&m=6&h=201&w=358&b=%23FFFFFFFF&l=f&o=t&x=839&y=615&aim=true
Preview:	II.. ...$..o.N.K..=wv.....f.....$..B.....$..B.....7.....WMPHOTO..F.q.e..0.....PPZ.EE.....,M..... .....UUUU.....^....7.+. .Q.'<. .I...m.c....U..#_....&.05Q.I.F.....?..^.Rh..@BZF.M..~Y&...6H...4.d.J.uh..Fe,l.f.h...J..`..9..._.b.E.6...w.u$.5.H.....2.....;.E..X.k..`.....!s...A..b...C.....$T.|.p..[#..."'-.8.....uOE?..BX. ..T.c.Lv+...V..-3...P..&...3v.P*H.....d..%%..0P@.G$U.aEo.2!mx.....IB...N....V[..l/'.K}..Z....[D75.7.I&....A)...H.@..T...\.:eL[b.(o.. ...$C..5.....b..M..P.J...7."y..[X.lO0.c.....L.!. ..6..y.....f.....`..R&:.IZ...E.8..S..J...."...S>k5.<...A....\U.....i.....sB.E..}...h..X.....@..p.Z.y.....j...F.[...5J.?...6..P..}..8.aJW.h.#.\|dD.;...&.d7n...1]...w}.B)J. .%...j+..bB.=$..g.).F...;.k<g.W..m.P.>....-.>.TD.j.....p...8...D.v.....K_...B.U.*HO...FFL .....D..he.3k.I.).zKmkFJ.....J.....]+^..M.....T.s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\RE4HSnu[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1600 x 600, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	311450
Entropy (8bit):	7.989164130461453
Encrypted:	false
SSDEEP:	6144:2syidI/CD7ekr1uvTPuPpH/OT2sLWGw2xjKAHjcNDjhH/PA+Z:2syiuaDTiPux/OT2sLWSdKijcthRZ
MD5:	ECB5CD0223EC4CE836DA21E165FAA4EC
SHA1:	7BF0948C610B6CF9853E5CF873DA24423AAFF362
SHA-256:	073A206ED139701FCEEDF118E58FB154373E259104804D7E39F2190B285E09B7
SHA-512:	AB5AE1539391C5E7915C7C8CEC15059DDC1192EEBC0FF823FBE0DBA262D1D9930EBF8AFCFB683E3B6936C5F5DD0C99900BCB21C975E0C5AC34AC71417770FB1C
Malicious:	false
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4HSnu?ver=0caa&q=0&m=8&h=600&w=1600&b=%23FFFFFFFF&l=f&x=0&y=0&s=1898&d=712&aim=true
Preview:	.PNG.....IHDR...@...X.....:.*B....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^....$Gy6.g.'...6...SB..D.....9'c..mL.....8.....s.BY..t...9.N..4.zk.O.e/I....D...Su..w..@&.... .....D.x.....]D..".C .R...s..A>....48..\.@`...C..:.s\|.r..\.....Sq..4{..."*F..M."....^>.....y<..#.1.o....S.X^.....x....9.u..f..va.....8{#<'.\|...`..._v...c+.....-tjq.....'.../Q^...F ..u#.~%.j.N.EG.....rI.j..C.$..|5.v....!"""""""".S...(/...u.U...#.t.b.W"`..."Z.j....~<....t<.k....XDDDDDDDDDt.H.#.t1...".h.iT....K...Vv7*nY...C....^-...P..C..C.....:.8.....N.ny...]p....M.R. .|.b.O.....[>..JF.\z.:..jA.....8..]s$O.Zz|..!"""""""""..G.S.@9....;aT..B.0.F..6#R...H....d..@.7.....8.....t|0.BDDDDDDDDD...g.-N.....Cp.,...\..n...>.f.A...'3..<..O.#@..... ..L...w..tj 0.BDDDDDDDDD...N...&`/....J%.#q.f...s.m{*B..u.;...j. .A.Cm..t\.ky..9.N<.@.....h...)L ?.3..!.v.^%.....n....!R...`...@@-t... ...k.@._v. ..9.#..S..."""""""""""Z;*...(..w.*M.\XD.y8V...A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\RE4pndL[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 40 x 40, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1093
Entropy (8bit):	7.746658713530522
Encrypted:	false
SSDEEP:	24:sgiCBITQBLZ02PHSeJN3Z+BKkrT3miwuU9ML8b9:b7d0cHSeJNZszT3mzuUq8R
MD5:	D4AEAB6DF868DB6F8E33844B93EB3EC1
SHA1:	C152F4E01EE36E70431DB0A45F343A1E284F52C5
SHA-256:	A5357CE15116A6FEBF6D0EBA74C67A8643D3AB5F219FCA79C8F1765A36918715
SHA-512:	AE20E5C8E10A8632439D59BAC804A4383EACC5CBAFE88392BAB20CA47EBDC6F3AC97A2D564D4043A1B3C51F5ADCE66A7ACE7B3FEF7B3F3367A01BD36A5304802
Malicious:	false
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4pndL?ver=5217&q=90&m=6&h=40&w=40&b=%23FFFFFFFF&l=f&o=t&aim=true
Preview:	.PNG.....IHDR...(...(.....m....sRGB.....gAMA.....a.....pHYs.....o.d....IDATXG.M..G...uv.GW..5.....$xP.Uw.^.\<...C .I.. ..<x.+(...._.=K.*Btf...ww.g..{....w.h.6..Cu=. T.S.~.7k.1..c.1.....e....59...n-..v..Zr.C..\+..v.,d.T.9..YJM).B .h.~.....g....X..F.t.`...z...Y....kv...)..-.....hk..e..hc....(.....M.3E.Q..0r...R...Ya(....1^...._..r.../.<.S..qbki.-...?....U...:. .F.....r.@{...J...c...Zh....y<.<M...\...Yb.6.b.)....sL.U..P.....6B.).1D0....m.E,\2.R..n'.H.&...$GY*A .F..Q.W0DPV..E.N.Q.....O0HP..._..{..WLy.}.....?....a.x...f.$..\&$...8....yW. .}. T....z..]..x...<.....<Mz.....8.'...FU..o.;kW*..R.l.W@..T....M9`...w..Br.....r...=b.)....&..zxA.....j..."..N n..._H.}3x....9.xM..;bT0..o%..^m1.R.T.q%..*...Im.....g].o ...~B..... ....x ^.....B.x;.....%.B.. 4.f...n..M\....B...,.....C7....s.Z....."..\XN).X.G?...<....Z.....%?B.7..o..m.i~...n.....L.*H.1....S.3..%6..s...i2.A~`.("J..O...S..n.CD..#3..0,u3..8...9.....N!$..$.I

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\RE4pxBu[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 40 x 40, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	605
Entropy (8bit):	7.5199699153609325
Encrypted:	false
SSDEEP:	12:6v/7PqXuMxRUHNV7ROerL/EmNsgF8wUy+cghBZ+QXe0q1cg+SR:+RM7cbUen/d8BZxcKg1R
MD5:	2DCF76D4D92B70117E41CC5BE6B686A0
SHA1:	C18F5F4CF898EA6394098EE5C7DFB501E6385DEA
SHA-256:	148606900BB9E626F0C3EB03C5E258E219B5E32BACE51C574169A9A123D64189
SHA-512:	F03609219E9B2AF5F584D6D25E1EC6E053F43DDB26E037AC2491AF305AB6ECFDDEA610DEAC852728DA1918844C1AA030733B14EA62A9092EC2A95F9CB86104AB
Malicious:	false
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4pxBu?ver=eae5&q=90&m=6&h=40&w=40&b=%23FFFFFFFF&l=f&o=t&aim=true

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\RE4pxBu[1].png	
Preview:	.PNG.....IHDR...(...(.....&.p.....orNT..w.....sRGB.....IDATH.V].. ...D0...@.#...D ...@."........^x.x.qwf.....a.q`.?.....l...Gxh..{.....`,.l...E2..B,.....SF.c|T0.x.5c..."..[A..l..... 2.^_...jz.>.....<..m...|A.8..H._f..;[....I..CN...$d...n..J...pGFfST..\|..4...5..9...?Q#2..f".W;... .....a.^.[2i..4..c... >."$....i.g.).+V.....d.x...h.|ta3...\...R..OQ....l...T.|..C.*....].;..>..c.. P.z.V...r....zbmB.....(.|..e-.?..0Yr.h.....p..w.>+/....e.... JS....U...H...l..?...E.4.}.;....M.c.{....'9..!8.DOA."(..Q.q....- ..Q5....kO75m..Wn...w.U.....r....,.D.z.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\RE4sQDc[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 40 x 40, 2-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	163
Entropy (8bit):	5.471990178621621
Encrypted:	false
SSDEEP:	3:yionv//thPlVXnblpNgpBhV0iMVEeo+kMlsLtsWsoHdaRr3dO07I6F7CXjp:6v/lhPDCdV0TeksRlsSdUtO07IOCTp
MD5:	B2E9EB438C6B233684822F9CFD7D6499
SHA1:	F3F213AE98CF6890DA39692815349DA6FC2B70CD
SHA-256:	821EBFBAD9774A7B858E9A73134E6EECD63EA6CC25B53E7163FA48F4276419C3
SHA-512:	711F9F9CD7E04096FC632B8CE678AE67718E5AD4D46981F7A2A462AAF1EED4F461BF0852D6C1EE7046E3AB4F4F74FAF30B503A04C243DD2CD199FD6FC4CA04BD
Malicious:	false
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4sQDc?ver=30c2&q=90&m=6&h=40&w=40&b=%23FFFFFFFF&l=f&o=t&aim=true
Preview:	.PNG.....IHDR...(...(.....P.....PLTE.....tRNS...9.....orNT..w.....sRGB.....)IDAT..c`.....E.H|..L.....U ...?.....0G.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\accountproperties[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):	4124
Entropy (8bit):	4.876744080458106
Encrypted:	false
SSDEEP:	48:U+dSYux+JjRNyJqaRBRvg0BdqVDunV7EogCDajg6a7tQfDEWURJgPuyaHuB:iCZYqaRQkColfe86aBXcaA
MD5:	87BB8E3F710FB38EFE61ACE9A01179F4
SHA1:	CF08F6C4360F77CCBEDA5E22BF3E8C8A7D24E514
SHA-256:	EEB2767FD675DE3D846F7C4D2B32105A850CDBEF5C3E417886F606AA3F05BCA9
SHA-512:	3F936B6F70D008960A5183068D4C4E5722AB7AF06D0332E206470E6CF45E8D302413B6F7408797C0C1D77B19C4E25D124BAAA8B242774008521654C8E66DAC25
Malicious:	false
IE Cache URL:	http://https://accdn.lpsnmedia.net/api/account/60270350/configuration/setting/accountproperties/?cb=lpCb64195x20500
Preview:	lpCb64195x20500([{"id":"messaging.ios.sdk.min.version","createdDate":"2017-01-10 04:11:41","type":2,"propertyValue":{"value":"1.1.36"},"deleted":false},{"id":"messaging.audio.sharing.enabled","createdDate":"2018-05-13 02:02:09","modifiedDate":"2018-11-14 08:32:03","type":2,"propertyValue":{"value":"false"},"deleted":false},{"id":"messaging.ios.logs.settings","createdDate":"2017-01-10 04:11:41","type":4,"propertyValue":{"value":{"level":"WARNING","minLogLevel":"INFO","randomFactor":1000.0,"maxEvents":50.0,"maxPendingEventsRequests":10.0}},"deleted":false},{"id":"unified.window.fallback.to.first.party.cookies","createdDate":"2019-11-20 03:10:29","type":2,"propertyValue":{"value":"false"},"deleted":false},{"id":"le.agent.widgetSdk.allowMicrophoneCamera","createdDate":"2019-08-19 04:03:07","type":2,"propertyValue":{"value":"false"},"deleted":false},{"id":"le.site.automotive.conversation.topics","createdDate":"2019-10-11 09:13:33","type":3,"propertyValue":{"value":[]},"deleted":false},{"id"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\cartcount[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1283
Entropy (8bit):	4.393500974386876
Encrypted:	false
SSDEEP:	12:KPgkrfXKLf7fcabNBGFMpYMNwy+Mz4zMGgZv4c0EgtiQ5FgWyb0gDIgdcZPx+Ydg:KPv6HUY5+yAZFAXJqiXZXTMK
MD5:	1BF3F6D72753254D68A4A8C99DB850AD
SHA1:	E98B92CFF496817E3D5E6CD117F06BEEFAAD3E5F
SHA-256:	68D929A10C3CD609B936B50A541533994B044B38558A33530FF45D1B420CC07E
SHA-512:	C2F17E5861E800E32F3AC3DEA7424384E82B2F27B79C14D24686C286D5A6559CABDABB6A58DF9125334E196CC7D3116B583B3AE1D9AE6711AB21F9F4B06AF20
Malicious:	false
Preview:	.....<!DOCTYPE html>..<html>..<head>.. <title>title</title>..</head>..<body>.. <script>.. function getCartItemCountFromCookie() {.. var name = 'cartItemCount=';.. var allCookies = document.cookie.split(';');.. for (var i = 0; i < allCookies.length; i++) {.. var c = allCookies[i];.. while (c.charAt(0) === ' ') {.. c = c.substring(1);.. }.. if (c.indexOf(name) === 0) {.. return c.substring(name.length, c.length);.. }.. }.. return 0;.. }.... var count = getCartItemCountFromCookie();.... var parentHost = '';.. var parentOriginProtocol = '';.. var parentOrigin = '';.. try {.. parentHost = parent.location.hostname || '';.. parentOriginProtocol = parent.location.protocol;.. parentOrigin = parent.location.origin;.. } catch {..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\dnserror[1]	
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=9002
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. <div id="contentContainer" class="mainContent">.. <div id="mainTitle" class="title">Can’t reach this page</div>.. <div class="taskSection" id="taskSection">.. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG........IHDR...............ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W.U.............W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~...b..$..s...7tRNS.a.o(,.s....e......q*...................................F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.......D.>..LpX=f.M...H4........=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 6 icons, 128x128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsLsQZp:nfgyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD0
Malicious:	false
IE Cache URL:	http://https://c.s-microsoft.com/favicon.ico?v2
Preview:	..............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(....................(....................................."P..."""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""" ...3333333333333333333333333333333""""""""""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\me[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	10273
Entropy (8bit):	5.43934371728387

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\me[1].htm	
Encrypted:	false
SSDEEP:	192:FDH1n+7Xr+cHEzFQD6Ds35b05e58ITZSTXh7gk0yi4BwL+md8:FE7XrUJds35bd8cAeju
MD5:	EB97CD55185A5AF641EA1DFF8A5BA028
SHA1:	28724529363E3934068B72DD4F61A227A0E8FA3A
SHA-256:	61080C13D6AC6A115D97FC4B1BDB637023327B29E7D9EDC908056497613CDBCF
SHA-512:	DF6C227463555F09030557F066DE9EE9731313C95F07C79D4C2DF7A9B41BBD00A46607F0EA6170F32C4D6896257C7813D1790E9AF85B3BB9614E66C195EFF617
Malicious:	false
Preview:	Copyright (C) Microsoft Corporation. All rights reserved. --><!DOCTYPE html> ServerInfo: SJ1PPF64AE4F597 2020.10.23.21.27.05 Live1 Unknown LocVer:0 --> P reprocessInfo: azbldrun:AzBuildW2-Ha13, 2020-11-23T03:56:21.9041428-08:00 - Version: 16,0,28799,16 --> RequestLCID: 1033, Market:EN-US, PrefCountry: US, LangLCID: 1033, LangISO: EN --><html dir="ltr" lang="EN-US"><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"/><base href="https://login.live.com/pp1600/"/><noscript><meta http-equiv="Refresh" content="0; URL=https://login.live.com/jsDisabled.srf?mkt=EN-US&lc=1033&uaid=deeb084a423f45f75b4520 42871f7db1"/>Microsoft account requires JavaScript to sign in. This web browser either does not support JavaScript, or scripts are being blocked. To find out w hether your browser supports JavaScript, or to allow scripts, see the browser's online help.</noscript><title>Windows Live ID</title><meta name="robots" content="none" /><meta name="PageID" co

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):	4.2887395101637535
Encrypted:	false
SSDEEP:	3:oVXVPwXf8+gRIpEmW8JOGXnFPwXf8+gRIU7n:o99+gnHqN+gf7
MD5:	9744D25756B1A4D7F1B7E180B0FDB093
SHA1:	8699DE5BFD2927B52446D8DA93C2FCFF93559C08
SHA-256:	D5A9568D63423BEBF0F0AF829B297C29D87679AEF921F68607C5CC160E60D2A3
SHA-512:	8FBC710484CE40FD88EA54698944F9DCC989D61FA123EC64C2236BE2848DF423828FCDEE74809DBB8D86D66269AD5AF65356E3E3C1891B08580B61F90BA8C48
Malicious:	false
Preview:	[2020/11/28 12:03:30.234] Latest deploy version: ..[2020/11/28 12:03:30.234] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF67E3D37EE042C482.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38819
Entropy (8bit):	0.37519102320376707
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwO9lwe9l2g9l2A9l/Qe:kBqoxKAuvScS+hftsQIQIqnTqngqnN
MD5:	71695F2F904472CD749B72AEA42F39A7
SHA1:	A900AA3E691B56A3E5C44C9EC7725CECC494B0CC
SHA-256:	8901E6AE0A2C8E43ADF9BB54C64481361E96AB3D0223D3E7402E5B52B0ADAA73
SHA-512:	D37811CF55EF8E94A63075048923A6FAFDF5F68F8575221B5A8C9072A6BF1CDF5FC445759BE5CA0535AA44D7086106518CC769E497BBB149D64A42EA050D98BA
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF68A6692B1F72E627.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38819
Entropy (8bit):	0.3750702072132498
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwhT9lwhT9l2hl9l2hlq:kBqoxKAuvScS+CkuHLILtnTtngtnN
MD5:	697443054C1326FFD928395E7957DBB4
SHA1:	19F42AAC083D20BF78C6C608705F1EDB23602BF6
SHA-256:	B184DD0D6AE064B493313E0E3F14A708DB4EAC779BD01BD3B933E0B3149A3BB3
SHA-512:	F5C3748F0CE320BE9164BE5142FDE79373247CE8DF89CF9B405D661E2F3D7AEF972091897CA94FA71649BB7CF537182BB63C2A4F3634C71FDAB599087F70D940
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF724610E3F111291D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.40717595158418785
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loxY9loxo9lWxsPXlO:kBqoItrC8
MD5:	4D99D8555561CF809B16CFA99C8AD583
SHA1:	6F25DEB943BD328B2641CDCD925AD765B082CCB6
SHA-256:	2C59C177C820A02A0917127545CBCC232BB6BA5CD76E219E0002DBEBD894F7B0
SHA-512:	9AFE819D88C458AC1CDCE70BA845394ED2B9E17AF96DABEACE092C26E5F1EC07E51B081139FE057984176EC7F8ECBAF89C44DCD867469859E263FDFC6159C 83
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF859C4A3D90DE0E8D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39465
Entropy (8bit):	0.537612628251998
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+bVHuVTQAk2JtzQAk2JtjQAk2JtI:kBqoxKAuqR+bVHuVTFk2TzFk2TjFk2TI
MD5:	B250B14ED100D7B7BAC11998E21ACFD5
SHA1:	2BC04E37C389CC8F62FA42B2F04310EC69A92716
SHA-256:	33BC5E524C51597414064A10A0F2B12E8C00917186887795C1E69A2CE9DDCA35
SHA-512:	DF12DF2646E0AD2A9A8FBC4CEF9C6EB55ACAB6C04084E1D44FCBDA2A725F891BABC7EEFA46765500BFEA67D84D77AC7D27865ACF45F307CCFF8D5E18DF68 5331
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF8FBA83EEC5070EA3.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.40799332454640924
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loM9loc9lWKjOEKn:kBqoI3Rp
MD5:	7D907A0ADEC3A16E9B32EF82B5387DA7
SHA1:	AAEBDABA44D737BFACFB9C1610036657D5674E9C
SHA-256:	68DC046DEB8D243DB9AA9FA93F4AFBD203EE008264D117D93F069A4A61BFB992
SHA-512:	DE186967547E11169BE80C33F4C22578C27197C03A6A3769D20D9A23D83844143C41BAEBDF23BCAC13852E7C53A41972FE4740F404F80C74491ED4A4EB753A9C
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFDB45CE98218A909C.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4086550906168016
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lod9lo99lWmKrca:kBqoIGYmKrca
MD5:	DB6F11D2CC778930F26E1128D8E9E042
SHA1:	7FE60127462EB574610BEB2F34524066C4CFEBC9

C:\Users\user\AppData\Local\Temp\~DFDB45CE98218A909C.TMP	
SHA-256:	FEB16B6292C9D989B942D8B68369227A0B3933A66376F79FD7FD9EE9ED2F0B4D
SHA-512:	D02EB8B0ED1D3BB4AD398D2F24FCBB9E276A3E390E57DE4F7B31289CFCBDBC09B7804B22E6599BB0FE144A077C938BD3F11E8AA11361CDB5CC937244CBBD(6C8
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.978693137770206
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	2tsY1gtYQe.exe
File size:	193024
MD5:	75dd85a6d1389e53fb125ebd9d2711a3
SHA1:	39d33f5c7aa2364f0f345f566946758ad3af80d4
SHA256:	2b120acc21bb146f94d229b7efeef732ab31dc9874fa00174f61e7673982a309
SHA512:	1a0ac909fa0ad554dc2972679c5f8a0bc944d435595eb9de227ff2f6fa70cffdfd05857df1cec16d11589550f80d3f004c6d471e9a291b50ff0e466e66493116
SSDEEP:	3072:Y4cYSAmimVnYVVfoaxG2JgvlsJU/GLDUdx6SklQWW:npWVVneVgcGGgsJHYrP
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Ysi.8.:.8.:.8.:.j.:.8.:.j.:.8.:.j.:"8.:..f:.8.:.8.:.8.:.j.:.8.:.j.:.8.:.j.:.8.:Rich.8.:.....PE..L...&TD].....<.

File Icon

Icon Hash:	acac96eee2fae278

Static PE Info

General

Entrypoint:	0x405003
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x5D445426 [Fri Aug 2 15:17:58 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	146e7fadf37dc1a6aabb0951b715f04e

Entrypoint Preview

Instruction
call 00007FA70CA4EE1Bh
jmp 00007FA70CA4634Dh
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
xor ecx, ecx
cmp eax, dword ptr [0042A0E8h+ecx*8]
je 00007FA70CA464E5h
inc ecx
cmp ecx, 2Dh
jc 00007FA70CA464C3h
lea ecx, dword ptr [eax-13h]
cmp ecx, 11h
jnbe 00007FA70CA464E0h
push 0000000Dh
pop eax
pop ebp
ret
mov eax, dword ptr [0042A0ECh+ecx*8]
pop ebp
ret
add eax, FFFFFF44h
push 0000000Eh
pop ecx
cmp ecx, eax
sbb eax, eax
and eax, ecx
add eax, 08h
pop ebp
ret
call 00007FA70CA49685h
test eax, eax
jne 00007FA70CA464D8h
mov eax, 0042A250h
ret
add eax, 08h
ret
call 00007FA70CA49672h
test eax, eax
jne 00007FA70CA464D8h
mov eax, 0042A254h
ret
add eax, 0Ch
ret
mov edi, edi
push ebp
mov ebp, esp
push esi
call 00007FA70CA464B7h
mov ecx, dword ptr [ebp+08h]
push ecx
mov dword ptr [eax], ecx
call 00007FA70CA46457h
pop ecx
mov esi, eax
call 00007FA70CA46491h
mov dword ptr [eax], esi
pop esi
pop ebp
ret
mov edi, edi
push ebp
mov ebp, esp

Instruction
sub esp, 4Ch
mov eax, dword ptr [0042A260h]
xor eax, ebp
mov dword ptr [ebp-04h], eax
push ebx
xor ebx, ebx
push esi
mov esi, dword ptr [ebp+08h]
push edi
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-1Ch], ebx
mov dword ptr [ebp-20h], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-24h], ebx
mov dword ptr [ebp-4Ch], esi
mov dword ptr [ebp-48h], ebx
cmp dword ptr [esi+14h], ebx

Rich Headers

Programming Language:	• [C] VS2008 build 21022 • [LNK] VS2008 build 21022 • [ASM] VS2008 build 21022 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [C++] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x292c8	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4c9000	0x4488	.rsrc
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	0x25000	0x1cc	.rdata
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
.text	0x1000	0x23abd	0x23c00	False	0.702237215909	data	7.29958716191	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x25000	0x4d2e	0x4e00	False	0.406951121795	data	5.42739065236	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x2a000	0x49e7a8	0x1e00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x4c9000	0x4488	0x4600	False	0.505859375	data	4.93620960984	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x4cb870	0x134	data		
RT_CURSOR	0x4cb9c0	0x130	data		
RT_CURSOR	0x4cbaf0	0xf0	data		
RT_CURSOR	0x4cbbe0	0x10a8	data		
RT_ICON	0x4c92b0	0x25a8	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_STRING	0x4ccdf0	0x3e4	data		
RT_STRING	0x4cd1d8	0x2aa	data		
RT_GROUP_CURSOR	0x4cb9a8	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x4ccc88	0x30	data		
RT_GROUP_ICON	0x4cb858	0x14	data	English	United States
RT_VERSION	0x4cccb8	0x134	data		

Imports

DLL	Import
KERNEL32.dll	SetPriorityClass, WritePrivateProfileStructA, TlsGetValue, CompareFileTime, GetUserDefaultLCID, _lcreat, SetTapeParameters, GetProcessPriorityBoost, GetTickCount, GetSystemTimeAsFileTime, ReadConsoleW, ActivateActCtx, TerminateThread, Sleep, IsDBCSLeadByte, ReadFile, CompareStringW, lstrlenW, SetThreadPriority, DeactivateActCtx, EnumResourceNamesW, GetPrivateProfileIntW, IsDBCSLeadByteEx, GetProcAddress, GetTapeStatus, SetVolumeLabelW, GetConsoleDisplayMode, SearchPathA, DisableThreadLibraryCalls, GetLocalTime, LoadLibraryA, CreateSemaphoreW, LocalAlloc, SetConsoleDisplayMode, AddAtomW, GetPrivateProfileStructA, GetModuleHandleA, VirtualProtect, CloseHandle, lstrcpyW, lstrcpyA, GetNamedPipeHandleStateW, GetThreadContext, WideCharToMultiByte, InterlockedIncrement, InterlockedDecrement, InterlockedCompareExchange, InterlockedExchange, MultiByteToWideChar, InitializeCriticalSection, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, GetLastError, HeapFree, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, HeapReAlloc, HeapAlloc, GetCommandLineA, GetStartupInfoA, GetCPInfo, RtlUnwind, RaiseException, LCMapStringW, LCMapStringA, GetStringTypeW, GetCurrentProcessId, GetModuleHandleW, TlsAlloc, TlsSetValue, TlsFree, SetLastError, GetCurrentThreadId, GetFileType, CreateFileA, HeapCreate, VirtualFree, VirtualAlloc, GetACP, GetOEMCP, IsValidCodePage, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, SetHandleCount, QueryPerformanceCounter, GetStringTypeA, HeapSize, GetLocaleInfoA, EnumSystemLocalesA, IsValidLocale, InitializeCriticalSectionAndSpinCount, SetStdHandle, GetConsoleCP, GetConsoleMode, SetFilePointer, SetEndOfFile, GetProcessHeap, GetLocaleInfoW, FlushFileBuffers, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW
GDI32.dll	GetCharWidthA

Version Infos

Description	Data
ProductVer	2.0.9.29
FileV	1.0.2.37
Translations	0x0255 0x029d

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

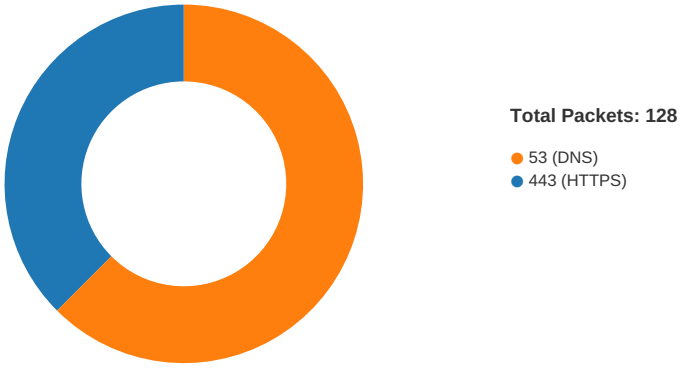
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/28/20-12:03:32.248270	ICMP	399	ICMP Destination Unreachable Host Unreachable			185.212.45.15	192.168.2.4
11/28/20-12:03:32.248296	ICMP	399	ICMP Destination Unreachable Host Unreachable			185.212.45.15	192.168.2.4
11/28/20-12:03:32.248304	ICMP	399	ICMP Destination Unreachable Host Unreachable			185.212.45.15	192.168.2.4
11/28/20-12:03:32.248311	ICMP	399	ICMP Destination Unreachable Host Unreachable			185.212.45.15	192.168.2.4
11/28/20-12:03:36.936269	ICMP	399	ICMP Destination Unreachable Host Unreachable			185.212.45.15	192.168.2.4
11/28/20-12:03:36.936308	ICMP	399	ICMP Destination Unreachable Host Unreachable			185.212.45.15	192.168.2.4
11/28/20-12:03:39.984175	ICMP	399	ICMP Destination Unreachable Host Unreachable			185.212.45.15	192.168.2.4
11/28/20-12:03:39.984205	ICMP	399	ICMP Destination Unreachable Host Unreachable			185.212.45.15	192.168.2.4

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/28/20-12:03:44.016154	ICMP	399	ICMP Destination Unreachable Host Unreachable			185.212.45.15	192.168.2.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 12:02:22.093893051 CET	49756	443	192.168.2.4	151.101.1.192
Nov 28, 2020 12:02:22.094125986 CET	49757	443	192.168.2.4	151.101.1.192
Nov 28, 2020 12:02:22.112904072 CET	443	49756	151.101.1.192	192.168.2.4
Nov 28, 2020 12:02:22.112955093 CET	443	49757	151.101.1.192	192.168.2.4
Nov 28, 2020 12:02:22.113087893 CET	49756	443	192.168.2.4	151.101.1.192
Nov 28, 2020 12:02:22.114866018 CET	49757	443	192.168.2.4	151.101.1.192
Nov 28, 2020 12:02:22.115542889 CET	49756	443	192.168.2.4	151.101.1.192
Nov 28, 2020 12:02:22.116225004 CET	49757	443	192.168.2.4	151.101.1.192
Nov 28, 2020 12:02:22.134469032 CET	443	49756	151.101.1.192	192.168.2.4
Nov 28, 2020 12:02:22.134984016 CET	443	49757	151.101.1.192	192.168.2.4
Nov 28, 2020 12:02:22.135691881 CET	443	49756	151.101.1.192	192.168.2.4
Nov 28, 2020 12:02:22.136437893 CET	49756	443	192.168.2.4	151.101.1.192
Nov 28, 2020 12:02:22.136492014 CET	443	49756	151.101.1.192	192.168.2.4
Nov 28, 2020 12:02:22.136571884 CET	443	49756	151.101.1.192	192.168.2.4
Nov 28, 2020 12:02:22.136632919 CET	49756	443	192.168.2.4	151.101.1.192
Nov 28, 2020 12:02:22.136639118 CET	443	49757	151.101.1.192	192.168.2.4
Nov 28, 2020 12:02:22.136754990 CET	443	49757	151.101.1.192	192.168.2.4
Nov 28, 2020 12:02:22.136801958 CET	443	49757	151.101.1.192	192.168.2.4
Nov 28, 2020 12:02:22.136832952 CET	49757	443	192.168.2.4	151.101.1.192
Nov 28, 2020 12:02:22.136888027 CET	49757	443	192.168.2.4	151.101.1.192
Nov 28, 2020 12:02:22.136895895 CET	49757	443	192.168.2.4	151.101.1.192
Nov 28, 2020 12:02:22.155102968 CET	49757	443	192.168.2.4	151.101.1.192
Nov 28, 2020 12:02:22.155411005 CET	49757	443	192.168.2.4	151.101.1.192
Nov 28, 2020 12:02:22.155766964 CET	49757	443	192.168.2.4	151.101.1.192
Nov 28, 2020 12:02:22.174334049 CET	443	49757	151.101.1.192	192.168.2.4
Nov 28, 2020 12:02:22.174364090 CET	443	49757	151.101.1.192	192.168.2.4
Nov 28, 2020 12:02:22.174559116 CET	49757	443	192.168.2.4	151.101.1.192
Nov 28, 2020 12:02:22.174953938 CET	443	49757	151.101.1.192	192.168.2.4
Nov 28, 2020 12:02:22.174973011 CET	443	49757	151.101.1.192	192.168.2.4
Nov 28, 2020 12:02:22.174988031 CET	443	49757	151.101.1.192	192.168.2.4
Nov 28, 2020 12:02:22.175004005 CET	443	49757	151.101.1.192	192.168.2.4
Nov 28, 2020 12:02:22.175019979 CET	443	49757	151.101.1.192	192.168.2.4
Nov 28, 2020 12:02:22.175040007 CET	443	49757	151.101.1.192	192.168.2.4
Nov 28, 2020 12:02:22.175055981 CET	443	49757	151.101.1.192	192.168.2.4
Nov 28, 2020 12:02:22.175072908 CET	443	49757	151.101.1.192	192.168.2.4
Nov 28, 2020 12:02:22.175156116 CET	49757	443	192.168.2.4	151.101.1.192
Nov 28, 2020 12:02:22.175218105 CET	49757	443	192.168.2.4	151.101.1.192
Nov 28, 2020 12:02:22.175270081 CET	49757	443	192.168.2.4	151.101.1.192

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 12:02:22.186124086 CET	49756	443	192.168.2.4	151.101.1.192
Nov 28, 2020 12:02:22.188513041 CET	49756	443	192.168.2.4	151.101.1.192
Nov 28, 2020 12:02:22.190191031 CET	49757	443	192.168.2.4	151.101.1.192
Nov 28, 2020 12:02:22.205379963 CET	443	49756	151.101.1.192	192.168.2.4
Nov 28, 2020 12:02:22.205522060 CET	49756	443	192.168.2.4	151.101.1.192
Nov 28, 2020 12:02:22.207331896 CET	443	49756	151.101.1.192	192.168.2.4
Nov 28, 2020 12:02:22.207407951 CET	49756	443	192.168.2.4	151.101.1.192
Nov 28, 2020 12:02:22.207577944 CET	49756	443	192.168.2.4	151.101.1.192
Nov 28, 2020 12:02:22.249505043 CET	443	49757	151.101.1.192	192.168.2.4
Nov 28, 2020 12:02:22.269198895 CET	443	49756	151.101.1.192	192.168.2.4
Nov 28, 2020 12:02:22.999833107 CET	49767	443	192.168.2.4	143.204.215.116
Nov 28, 2020 12:02:23.003562927 CET	49768	443	192.168.2.4	143.204.215.116
Nov 28, 2020 12:02:23.016396999 CET	443	49767	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.016865969 CET	49767	443	192.168.2.4	143.204.215.116
Nov 28, 2020 12:02:23.018485069 CET	49767	443	192.168.2.4	143.204.215.116
Nov 28, 2020 12:02:23.020090103 CET	443	49768	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.020188093 CET	49768	443	192.168.2.4	143.204.215.116
Nov 28, 2020 12:02:23.020797968 CET	49768	443	192.168.2.4	143.204.215.116
Nov 28, 2020 12:02:23.035023928 CET	443	49767	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.035255909 CET	443	49767	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.035300016 CET	443	49767	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.035339117 CET	443	49767	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.035413980 CET	49767	443	192.168.2.4	143.204.215.116
Nov 28, 2020 12:02:23.035476923 CET	49767	443	192.168.2.4	143.204.215.116
Nov 28, 2020 12:02:23.037159920 CET	443	49767	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.037190914 CET	443	49768	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.037255049 CET	49767	443	192.168.2.4	143.204.215.116
Nov 28, 2020 12:02:23.037714958 CET	443	49768	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.037760019 CET	443	49768	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.037791014 CET	49768	443	192.168.2.4	143.204.215.116
Nov 28, 2020 12:02:23.037798882 CET	443	49768	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.037818909 CET	49768	443	192.168.2.4	143.204.215.116
Nov 28, 2020 12:02:23.039401054 CET	49768	443	192.168.2.4	143.204.215.116
Nov 28, 2020 12:02:23.042905092 CET	443	49768	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.042990923 CET	49768	443	192.168.2.4	143.204.215.116
Nov 28, 2020 12:02:23.049555063 CET	49768	443	192.168.2.4	143.204.215.116
Nov 28, 2020 12:02:23.049628019 CET	49767	443	192.168.2.4	143.204.215.116
Nov 28, 2020 12:02:23.049946070 CET	49768	443	192.168.2.4	143.204.215.116
Nov 28, 2020 12:02:23.066004038 CET	443	49768	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.066046000 CET	443	49767	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.066381931 CET	443	49768	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.066468000 CET	443	49768	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.066540956 CET	49768	443	192.168.2.4	143.204.215.116
Nov 28, 2020 12:02:23.066608906 CET	443	49767	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.067408085 CET	49767	443	192.168.2.4	143.204.215.116
Nov 28, 2020 12:02:23.067785025 CET	443	49768	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.067830086 CET	443	49768	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.067846060 CET	49768	443	192.168.2.4	143.204.215.116
Nov 28, 2020 12:02:23.067868948 CET	443	49768	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.067869902 CET	49768	443	192.168.2.4	143.204.215.116
Nov 28, 2020 12:02:23.067918062 CET	443	49768	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.067960978 CET	443	49768	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.067962885 CET	49768	443	192.168.2.4	143.204.215.116
Nov 28, 2020 12:02:23.067998886 CET	443	49768	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.068038940 CET	443	49768	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.068042994 CET	49768	443	192.168.2.4	143.204.215.116
Nov 28, 2020 12:02:23.068078041 CET	443	49768	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.068120956 CET	49768	443	192.168.2.4	143.204.215.116
Nov 28, 2020 12:02:23.068679094 CET	443	49768	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.068720102 CET	443	49768	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.068767071 CET	443	49768	143.204.215.116	192.168.2.4
Nov 28, 2020 12:02:23.068775892 CET	49768	443	192.168.2.4	143.204.215.116

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 12:01:54.767314911 CET	63153	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:01:54.802479029 CET	53	63153	8.8.8.8	192.168.2.4
Nov 28, 2020 12:01:55.496618032 CET	52991	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:01:55.532044888 CET	53	52991	8.8.8.8	192.168.2.4
Nov 28, 2020 12:01:56.181792974 CET	53700	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:01:56.209007978 CET	53	53700	8.8.8.8	192.168.2.4
Nov 28, 2020 12:01:56.877948999 CET	51726	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:01:56.905042887 CET	53	51726	8.8.8.8	192.168.2.4
Nov 28, 2020 12:01:58.092453003 CET	56794	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:01:58.119415998 CET	53	56794	8.8.8.8	192.168.2.4
Nov 28, 2020 12:01:59.257600069 CET	56534	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:01:59.284816027 CET	53	56534	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:19.147504091 CET	56627	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:19.186768055 CET	53	56627	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:20.227473021 CET	56621	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:20.283612967 CET	53	56621	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:20.384145975 CET	63116	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:20.421194077 CET	53	63116	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:20.856605053 CET	64078	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:20.870661020 CET	64801	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:20.875694036 CET	61721	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:20.877053022 CET	51255	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:20.878339052 CET	61522	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:20.878710985 CET	52337	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:20.893687010 CET	53	64078	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:20.894535065 CET	55046	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:20.897783995 CET	53	64801	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:20.899900913 CET	49612	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:20.914272070 CET	53	61721	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:20.914323092 CET	53	52337	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:20.915256023 CET	53	61522	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:20.924614906 CET	53	51255	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:20.932329893 CET	53	55046	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:20.943387985 CET	53	49612	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:22.037507057 CET	49285	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:22.090605021 CET	53	49285	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:22.248919964 CET	50601	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:22.284466028 CET	53	50601	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:22.306032896 CET	60875	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:22.363388062 CET	53	60875	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:22.398333073 CET	56448	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:22.441395044 CET	53	56448	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:22.615463972 CET	59172	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:22.654342890 CET	53	59172	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:22.944217920 CET	62420	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:22.953752041 CET	60579	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:22.987111092 CET	53	62420	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:22.997945070 CET	53	60579	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:23.016052961 CET	50183	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:23.061346054 CET	53	50183	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:23.405908108 CET	61531	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:23.452435017 CET	53	61531	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:23.515305042 CET	49228	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:23.542469025 CET	53	49228	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:30.305023909 CET	59794	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:30.332170963 CET	53	59794	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:31.021168947 CET	55916	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:31.048206091 CET	53	55916	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:31.699503899 CET	52752	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:31.726622105 CET	53	52752	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:32.576474905 CET	60542	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:32.603518963 CET	53	60542	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:41.851896048 CET	60689	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:41.887417078 CET	53	60689	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 12:02:42.340672970 CET	64206	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:42.346977949 CET	50904	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:42.376319885 CET	53	64206	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:42.384114981 CET	53	50904	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:42.795469046 CET	57525	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:42.833170891 CET	53	57525	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:43.149708033 CET	53814	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:43.187273026 CET	53	53814	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:43.529589891 CET	53418	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:43.556555033 CET	53	53418	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:43.952511072 CET	62833	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:43.987819910 CET	53	62833	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:44.181032896 CET	59260	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:44.216620922 CET	53	59260	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:44.412751913 CET	49944	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:44.439944029 CET	53	49944	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:45.016190052 CET	63300	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:45.051937103 CET	53	63300	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:45.668204069 CET	61449	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:45.703809977 CET	53	61449	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:46.081568003 CET	51275	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:46.108675003 CET	53	51275	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:49.105040073 CET	63492	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:49.144290924 CET	53	63492	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:50.099071980 CET	63492	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:50.137130022 CET	53	63492	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:51.099073887 CET	63492	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:51.134454012 CET	53	63492	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:53.115231991 CET	63492	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:53.150892973 CET	53	63492	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:57.131251097 CET	63492	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:57.166999102 CET	53	63492	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:58.925834894 CET	58945	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:58.952876091 CET	53	58945	8.8.8.8	192.168.2.4
Nov 28, 2020 12:02:58.954289913 CET	60779	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:02:58.997926950 CET	53	60779	8.8.8.8	192.168.2.4
Nov 28, 2020 12:03:02.731616020 CET	64014	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:03:02.768496990 CET	53	64014	8.8.8.8	192.168.2.4
Nov 28, 2020 12:03:04.755446911 CET	57091	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:03:04.792315006 CET	53	57091	8.8.8.8	192.168.2.4
Nov 28, 2020 12:03:05.886873960 CET	55904	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:03:05.922075987 CET	53	55904	8.8.8.8	192.168.2.4
Nov 28, 2020 12:03:06.026827097 CET	52109	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:03:06.064285994 CET	53	52109	8.8.8.8	192.168.2.4
Nov 28, 2020 12:03:06.522419930 CET	54450	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:03:06.533102036 CET	49374	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:03:06.553148985 CET	50436	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:03:06.555322886 CET	62605	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:03:06.568399906 CET	53	54450	8.8.8.8	192.168.2.4
Nov 28, 2020 12:03:06.576648951 CET	53	49374	8.8.8.8	192.168.2.4
Nov 28, 2020 12:03:06.588480949 CET	53	50436	8.8.8.8	192.168.2.4
Nov 28, 2020 12:03:06.614348888 CET	53	62605	8.8.8.8	192.168.2.4
Nov 28, 2020 12:03:06.689551115 CET	54256	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:03:06.725017071 CET	53	54256	8.8.8.8	192.168.2.4
Nov 28, 2020 12:03:06.946245909 CET	52189	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:03:06.983366013 CET	53	52189	8.8.8.8	192.168.2.4
Nov 28, 2020 12:03:07.221981049 CET	56131	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:03:07.257353067 CET	53	56131	8.8.8.8	192.168.2.4
Nov 28, 2020 12:03:07.563426018 CET	62992	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:03:07.598547935 CET	53	62992	8.8.8.8	192.168.2.4
Nov 28, 2020 12:03:08.104048967 CET	54432	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:03:08.139939070 CET	53	54432	8.8.8.8	192.168.2.4
Nov 28, 2020 12:03:29.756707907 CET	57227	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:03:29.793514013 CET	53	57227	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 12:03:30.851819992 CET	58383	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:03:30.894578934 CET	53	58383	8.8.8.8	192.168.2.4
Nov 28, 2020 12:03:38.148288965 CET	63136	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:03:38.175342083 CET	53	63136	8.8.8.8	192.168.2.4
Nov 28, 2020 12:03:39.607945919 CET	50911	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:03:39.643745899 CET	53	50911	8.8.8.8	192.168.2.4
Nov 28, 2020 12:03:45.005320072 CET	63409	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:03:45.040762901 CET	53	63409	8.8.8.8	192.168.2.4
Nov 28, 2020 12:04:06.003284931 CET	59185	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:04:06.040589094 CET	53	59185	8.8.8.8	192.168.2.4
Nov 28, 2020 12:04:06.255326986 CET	64236	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:04:06.290863037 CET	53	64236	8.8.8.8	192.168.2.4
Nov 28, 2020 12:04:06.373331070 CET	56157	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:04:06.412700891 CET	53	56157	8.8.8.8	192.168.2.4
Nov 28, 2020 12:04:06.701544046 CET	55601	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:04:06.702972889 CET	52984	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:04:06.704921961 CET	51141	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:04:06.706984043 CET	53610	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:04:06.710191011 CET	61247	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:04:06.738590002 CET	53	55601	8.8.8.8	192.168.2.4
Nov 28, 2020 12:04:06.743771076 CET	53	51141	8.8.8.8	192.168.2.4
Nov 28, 2020 12:04:06.743820906 CET	53	53610	8.8.8.8	192.168.2.4
Nov 28, 2020 12:04:06.745553970 CET	53	61247	8.8.8.8	192.168.2.4
Nov 28, 2020 12:04:06.746324062 CET	53	52984	8.8.8.8	192.168.2.4
Nov 28, 2020 12:04:07.220649004 CET	65165	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:04:07.264002085 CET	53	65165	8.8.8.8	192.168.2.4
Nov 28, 2020 12:04:07.712436914 CET	52076	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:04:07.749485016 CET	53	52076	8.8.8.8	192.168.2.4
Nov 28, 2020 12:04:07.939419031 CET	54903	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:04:07.974714041 CET	53	54903	8.8.8.8	192.168.2.4
Nov 28, 2020 12:04:08.433474064 CET	55045	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:04:08.469003916 CET	53	55045	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 28, 2020 12:02:20.856605053 CET	192.168.2.4	8.8.8.8	0xa7b0	Standard query (0)	assets.one store.ms	A (IP address)	IN (0x0001)
Nov 28, 2020 12:02:20.875694036 CET	192.168.2.4	8.8.8.8	0x6002	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)
Nov 28, 2020 12:02:20.878710985 CET	192.168.2.4	8.8.8.8	0x7b0a	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)
Nov 28, 2020 12:02:20.899900913 CET	192.168.2.4	8.8.8.8	0x37bd	Standard query (0)	microsoftw indows.112 .2o7.net	A (IP address)	IN (0x0001)
Nov 28, 2020 12:02:22.037507057 CET	192.168.2.4	8.8.8.8	0xbc33	Standard query (0)	publisher. liveperson.net	A (IP address)	IN (0x0001)
Nov 28, 2020 12:02:22.306032896 CET	192.168.2.4	8.8.8.8	0xae0a	Standard query (0)	lptag.live person.net	A (IP address)	IN (0x0001)
Nov 28, 2020 12:02:22.944217920 CET	192.168.2.4	8.8.8.8	0x8e21	Standard query (0)	accdn.lpsn media.net	A (IP address)	IN (0x0001)
Nov 28, 2020 12:02:22.953752041 CET	192.168.2.4	8.8.8.8	0x114d	Standard query (0)	static-assets.fs.liv eperson.com	A (IP address)	IN (0x0001)
Nov 28, 2020 12:02:23.405908108 CET	192.168.2.4	8.8.8.8	0xa78f	Standard query (0)	logincdn.m sauth.net	A (IP address)	IN (0x0001)
Nov 28, 2020 12:03:06.522419930 CET	192.168.2.4	8.8.8.8	0xe29a	Standard query (0)	assets.one store.ms	A (IP address)	IN (0x0001)
Nov 28, 2020 12:03:06.555322886 CET	192.168.2.4	8.8.8.8	0x8426	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)
Nov 28, 2020 12:03:06.689551115 CET	192.168.2.4	8.8.8.8	0xf737	Standard query (0)	microsoftw indows.112 .2o7.net	A (IP address)	IN (0x0001)
Nov 28, 2020 12:03:06.946245909 CET	192.168.2.4	8.8.8.8	0xd808	Standard query (0)	publisher. liveperson.net	A (IP address)	IN (0x0001)
Nov 28, 2020 12:03:07.563426018 CET	192.168.2.4	8.8.8.8	0xb021	Standard query (0)	accdn.lpsn media.net	A (IP address)	IN (0x0001)
Nov 28, 2020 12:03:30.851819992 CET	192.168.2.4	8.8.8.8	0x60d6	Standard query (0)	loadshemsp lot.xyz	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 28, 2020 12:03:45.005320072 CET	192.168.2.4	8.8.8.8	0x1c14	Standard query (0)	loadshemsplot.xyz	A (IP address)	IN (0x0001)
Nov 28, 2020 12:04:06.701544046 CET	192.168.2.4	8.8.8.8	0x5b6e	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)
Nov 28, 2020 12:04:06.704921961 CET	192.168.2.4	8.8.8.8	0x4621	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)
Nov 28, 2020 12:04:06.710191011 CET	192.168.2.4	8.8.8.8	0xe707	Standard query (0)	microsoftwindows.112.2o7.net	A (IP address)	IN (0x0001)
Nov 28, 2020 12:04:07.712436914 CET	192.168.2.4	8.8.8.8	0x88b8	Standard query (0)	accdn.lpsnmedia.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 28, 2020 12:02:20.893687010 CET	8.8.8.8	192.168.2.4	0xa7b0	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 28, 2020 12:02:20.897783995 CET	8.8.8.8	192.168.2.4	0x1222	No error (0)	consentdeliveryfd.azurefd.net	star-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 28, 2020 12:02:20.914272070 CET	8.8.8.8	192.168.2.4	0x6002	No error (0)	mem.gfx.ms	cdn.account.microsoft.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 28, 2020 12:02:20.914323092 CET	8.8.8.8	192.168.2.4	0x7b0a	No error (0)	mem.gfx.ms	cdn.account.microsoft.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 28, 2020 12:02:20.943387985 CET	8.8.8.8	192.168.2.4	0x37bd	No error (0)	microsoftwindows.112.2o7.net		15.237.136.106	A (IP address)	IN (0x0001)
Nov 28, 2020 12:02:20.943387985 CET	8.8.8.8	192.168.2.4	0x37bd	No error (0)	microsoftwindows.112.2o7.net		35.181.18.61	A (IP address)	IN (0x0001)
Nov 28, 2020 12:02:20.943387985 CET	8.8.8.8	192.168.2.4	0x37bd	No error (0)	microsoftwindows.112.2o7.net		15.237.76.117	A (IP address)	IN (0x0001)
Nov 28, 2020 12:02:22.090605021 CET	8.8.8.8	192.168.2.4	0xbc33	No error (0)	publisher.liveperson.net	publisher.livepersonk.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 28, 2020 12:02:22.090605021 CET	8.8.8.8	192.168.2.4	0xbc33	No error (0)	liveperson.map.fastly.net		151.101.1.192	A (IP address)	IN (0x0001)
Nov 28, 2020 12:02:22.090605021 CET	8.8.8.8	192.168.2.4	0xbc33	No error (0)	liveperson.map.fastly.net		151.101.65.192	A (IP address)	IN (0x0001)
Nov 28, 2020 12:02:22.090605021 CET	8.8.8.8	192.168.2.4	0xbc33	No error (0)	liveperson.map.fastly.net		151.101.129.192	A (IP address)	IN (0x0001)
Nov 28, 2020 12:02:22.090605021 CET	8.8.8.8	192.168.2.4	0xbc33	No error (0)	liveperson.map.fastly.net		151.101.193.192	A (IP address)	IN (0x0001)
Nov 28, 2020 12:02:22.363388062 CET	8.8.8.8	192.168.2.4	0xae0a	No error (0)	lptag.liveperson.net	lptag.liveperson.cotcdb.net.livepersonk.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 28, 2020 12:02:22.987111092 CET	8.8.8.8	192.168.2.4	0x8e21	No error (0)	accdn.lpsnmedia.net	accdn.lpsnmedia.livepersonk.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 28, 2020 12:02:22.997945070 CET	8.8.8.8	192.168.2.4	0x114d	No error (0)	static-assets.fs.liveperson.com	dh1y47vf5ttia.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 28, 2020 12:02:22.997945070 CET	8.8.8.8	192.168.2.4	0x114d	No error (0)	dh1y47vf5ttia.cloudfront.net		143.204.215.116	A (IP address)	IN (0x0001)
Nov 28, 2020 12:02:22.997945070 CET	8.8.8.8	192.168.2.4	0x114d	No error (0)	dh1y47vf5ttia.cloudfront.net		143.204.215.43	A (IP address)	IN (0x0001)
Nov 28, 2020 12:02:22.997945070 CET	8.8.8.8	192.168.2.4	0x114d	No error (0)	dh1y47vf5ttia.cloudfront.net		143.204.215.24	A (IP address)	IN (0x0001)
Nov 28, 2020 12:02:22.997945070 CET	8.8.8.8	192.168.2.4	0x114d	No error (0)	dh1y47vf5ttia.cloudfront.net		143.204.215.19	A (IP address)	IN (0x0001)
Nov 28, 2020 12:02:23.452435017 CET	8.8.8.8	192.168.2.4	0xa78f	No error (0)	logincdn.msauth.net	lgincdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 28, 2020 12:02:23.452435017 CET	8.8.8.8	192.168.2.4	0xa78f	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 28, 2020 12:03:06.568399906 CET	8.8.8.8	192.168.2.4	0xe29a	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 28, 2020 12:03:06.614348888 CET	8.8.8.8	192.168.2.4	0x8426	No error (0)	mem.gfx.ms	cdn.account.microsoft.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 28, 2020 12:03:06.725017071 CET	8.8.8.8	192.168.2.4	0xf737	No error (0)	microsoftwindows.112.2o7.net		15.237.136.106	A (IP address)	IN (0x0001)
Nov 28, 2020 12:03:06.725017071 CET	8.8.8.8	192.168.2.4	0xf737	No error (0)	microsoftwindows.112.2o7.net		35.181.18.61	A (IP address)	IN (0x0001)
Nov 28, 2020 12:03:06.725017071 CET	8.8.8.8	192.168.2.4	0xf737	No error (0)	microsoftwindows.112.2o7.net		15.237.76.117	A (IP address)	IN (0x0001)
Nov 28, 2020 12:03:06.983366013 CET	8.8.8.8	192.168.2.4	0xd808	No error (0)	publisher.liveperson.net	publisher.livepersonk.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 28, 2020 12:03:06.983366013 CET	8.8.8.8	192.168.2.4	0xd808	No error (0)	liveperson.map.fastly.net		151.101.1.192	A (IP address)	IN (0x0001)
Nov 28, 2020 12:03:06.983366013 CET	8.8.8.8	192.168.2.4	0xd808	No error (0)	liveperson.map.fastly.net		151.101.65.192	A (IP address)	IN (0x0001)
Nov 28, 2020 12:03:06.983366013 CET	8.8.8.8	192.168.2.4	0xd808	No error (0)	liveperson.map.fastly.net		151.101.129.192	A (IP address)	IN (0x0001)
Nov 28, 2020 12:03:06.983366013 CET	8.8.8.8	192.168.2.4	0xd808	No error (0)	liveperson.map.fastly.net		151.101.193.192	A (IP address)	IN (0x0001)
Nov 28, 2020 12:03:07.598547935 CET	8.8.8.8	192.168.2.4	0xb021	No error (0)	accdn.lpsnmedia.net	accdn.lpsnmedia.liveperson k.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 28, 2020 12:03:30.894578934 CET	8.8.8.8	192.168.2.4	0x60d6	No error (0)	loadshemsplot.xyz		185.219.220.94	A (IP address)	IN (0x0001)
Nov 28, 2020 12:03:45.040762901 CET	8.8.8.8	192.168.2.4	0x1c14	Server failure (2)	loadshemsplot.xyz	none	none	A (IP address)	IN (0x0001)
Nov 28, 2020 12:04:06.738590002 CET	8.8.8.8	192.168.2.4	0x5b6e	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 28, 2020 12:04:06.743771076 CET	8.8.8.8	192.168.2.4	0x4621	No error (0)	mem.gfx.ms	cdn.account.microsoft.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 28, 2020 12:04:06.745553970 CET	8.8.8.8	192.168.2.4	0xe707	No error (0)	microsoftwindows.112.2o7.net		15.237.136.106	A (IP address)	IN (0x0001)
Nov 28, 2020 12:04:06.745553970 CET	8.8.8.8	192.168.2.4	0xe707	No error (0)	microsoftwindows.112.2o7.net		35.181.18.61	A (IP address)	IN (0x0001)
Nov 28, 2020 12:04:06.745553970 CET	8.8.8.8	192.168.2.4	0xe707	No error (0)	microsoftwindows.112.2o7.net		15.237.76.117	A (IP address)	IN (0x0001)
Nov 28, 2020 12:04:07.749485016 CET	8.8.8.8	192.168.2.4	0x88b8	No error (0)	accdn.lpsnmedia.net	accdn.lpsnmedia.liveperson k.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 28, 2020 12:02:22.136571884 CET	151.101.1.192	443	192.168.2.4	49756	CN=liveperson.net, O="LivePerson, Inc.", L=New York, ST=New York, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Mar 27 04:17:26 CET 2020	Sun Mar 28 05:17:26 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 28, 2020 12:02:22.136801958 CET	151.101.1.192	443	192.168.2.4	49757	CN=liveperson.net, O="LivePerson, Inc.", L=New York, ST=New York, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Mar 27 04:17:26 CET 2020	Sun Mar 28 05:17:26 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
							Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
Nov 28, 2020 12:02:23.037159920 CET	143.204.215.116	443	192.168.2.4	49767	CN=fs.liveperson.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sun Aug 23 02:00:00 CEST 2020	Thu Sep 23 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
							Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
							Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
							Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Nov 28, 2020 12:02:23.042905092 CET	143.204.215.116	443	192.168.2.4	49768	CN=fs.liveperson.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sun Aug 23 02:00:00 CEST 2020	Thu Sep 23 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
							Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
							Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
							Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		

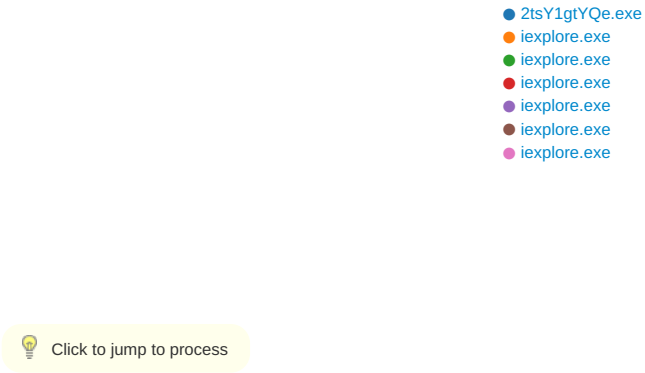
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Nov 28, 2020 12:02:23.493630886 CET	192.229.221.185	443	192.168.2.4	49774	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jul 20 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Tue Jul 20 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Nov 28, 2020 12:02:23.493733883 CET	192.229.221.185	443	192.168.2.4	49773	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jul 20 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Tue Jul 20 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Nov 28, 2020 12:03:07.033860922 CET	151.101.1.192	443	192.168.2.4	49804	CN=liveperson.net, O="LivePerson, Inc.", L=New York, ST=New York, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Mar 27 04:17:26 CET 2020 Wed Aug 19 02:00:00 CEST 2015	Sun Mar 28 05:17:26 CEST 2021 Tue Aug 19 02:00:00 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
Nov 28, 2020 12:03:07.036669970 CET	151.101.1.192	443	192.168.2.4	49805	CN=liveperson.net, O="LivePerson, Inc.", L=New York, ST=New York, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Mar 27 04:17:26 CET 2020 Wed Aug 19 02:00:00 CEST 2015	Sun Mar 28 05:17:26 CEST 2021 Tue Aug 19 02:00:00 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: 2tsY1gtYQe.exe PID: 6536 Parent PID: 6000

General

Start time:	12:01:59
Start date:	28/11/2020
Path:	C:\Users\user\Desktop\2tsY1gtYQe.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\2tsY1gtYQe.exe'
Imagebase:	0x400000
File size:	193024 bytes
MD5 hash:	75DD85A6D1389E53FB125EBD9D2711A3
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: 00000001.00000003.713969974.0000000003248000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.810687783.0000000002FCD000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.810749079.0000000002FCD000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.810673766.0000000002FCD000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.713981277.0000000003248000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.713850490.0000000003248000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.713931366.0000000003248000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.713804401.0000000003248000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.713880426.0000000003248000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.756942325.00000000030CB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000002.931050218.0000000002E50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.713643686.0000000003248000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.713707327.0000000003248000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6580 Parent PID: 800

General

Start time:	12:02:18
Start date:	28/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff61bab0000
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: 768 Parent PID: 6580

General

Start time:	12:02:19
Start date:	28/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6580 CREDAT:17410 /prefetch:2
Imagebase:	0x1110000
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

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: 5532 Parent PID: 800

General

Start time:	12:03:03
Start date:	28/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff61bab0000
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: 5504 Parent PID: 5532

General

Start time:	12:03:04
Start date:	28/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5532 CREDAT:17410 /prefetch:2
Imagebase:	0x1110000
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

Registry Activities

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

Analysis Process: iexplore.exe PID: 6824 Parent PID: 800

General

Start time:	12:03:29
Start date:	28/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff61bab0000

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: 6312 Parent PID: 6824

General

Start time:	12:03:29
Start date:	28/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6824 CREDAT:17410 /prefetch:2
Imagebase:	0x1110000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis