ID: 339453
Cookbook: browseurl.jbs
Time: 04:26:04
Date: 14/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

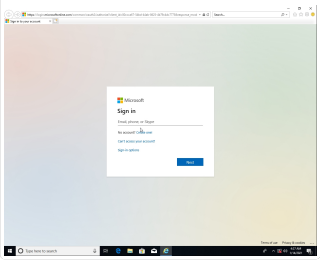
Analysis Report https://protection.office.com/campaigns

Overview

General Information

Sample URL:	http://https://protection.office.com/campaigns
Analysis ID:	339453

Most interesting Screenshot:



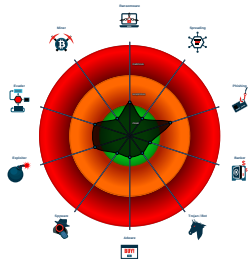
Detection

Score:	2
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- HTML body contains low number of …
- HTML title does not match URL
- Potential browser exploit detected (p…
- Submit button contains javascript call
- Very long cmdline option found, this…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6768 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6816 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6768 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - TokenBrokerCookies.exe (PID: 5484 cmdline: C:\Windows\system32\TokenBrokerCookies.exe <no_string> https://login.microsoftonline.com/ 0 tbauth://login.windows.net/?context=https%3A%2F%2Flogin.microsoftonline.com&request_nonce=AwABAAAAAAABAOz_AwD0_5mUgr2fSv4NxRRKhIfqZP9fUQosM2-hJX8votGQsH2PQuCecfPy-WPQWQ7eiFMW6_yA4NTsqZVOGf6tlSk0LBwgAA&rid=e376dce7-fc39-4390-87c3-8fadf9f10a00 ESTSUSERLIST %7b%22users%22%3a%5b%5d%7d login.microsoftonline.com / 0 183840 6162 30864677 1 MD5: 17F27A76AC8E9869C8F1BE286D88570A)
- **cleanup**

Malware Configuration

No configs have been found

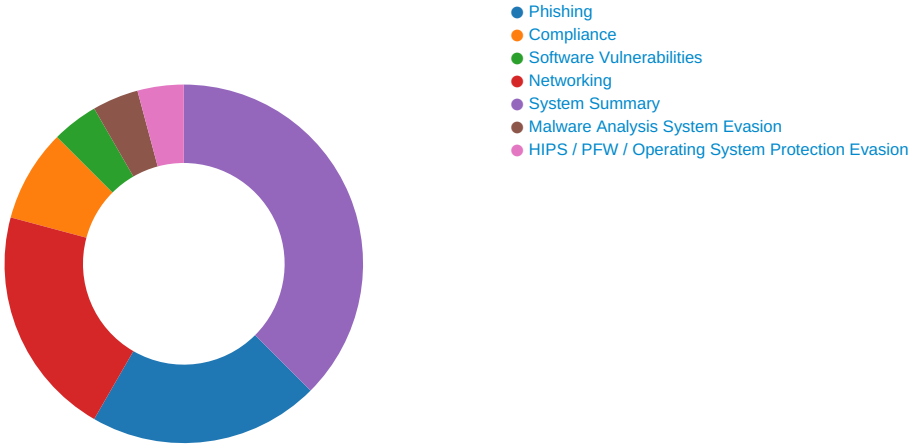
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



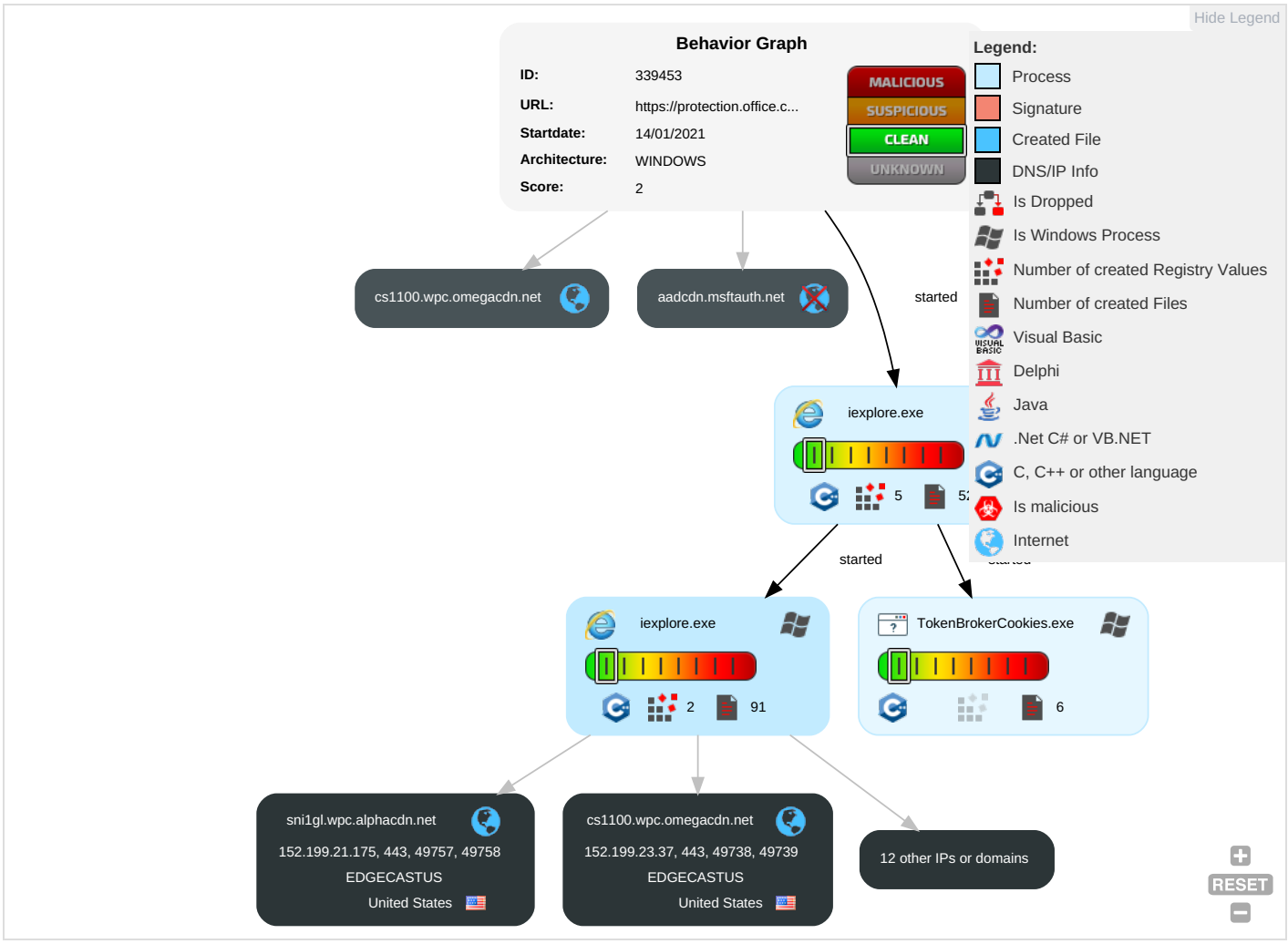
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Command and Scripting Interpreter 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partitior
Default Accounts	Scripting 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	Exploitation for Client Execution 1	Logon Script (Windows)	Logon Script (Windows)	Scripting 1	Security Account Manager	System Information Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

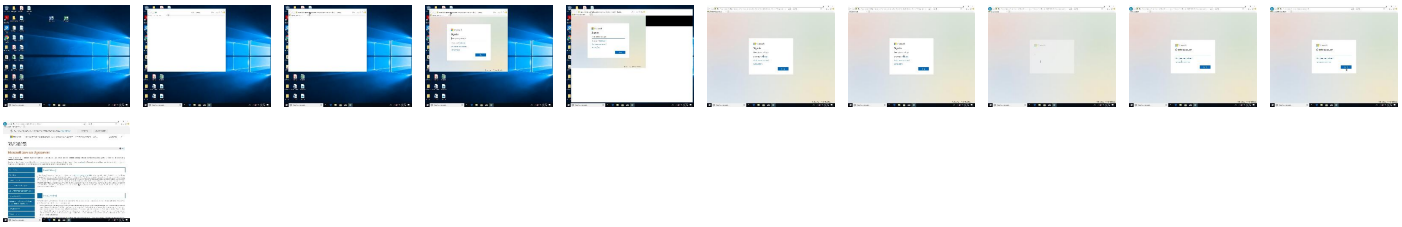
Behavior Graph

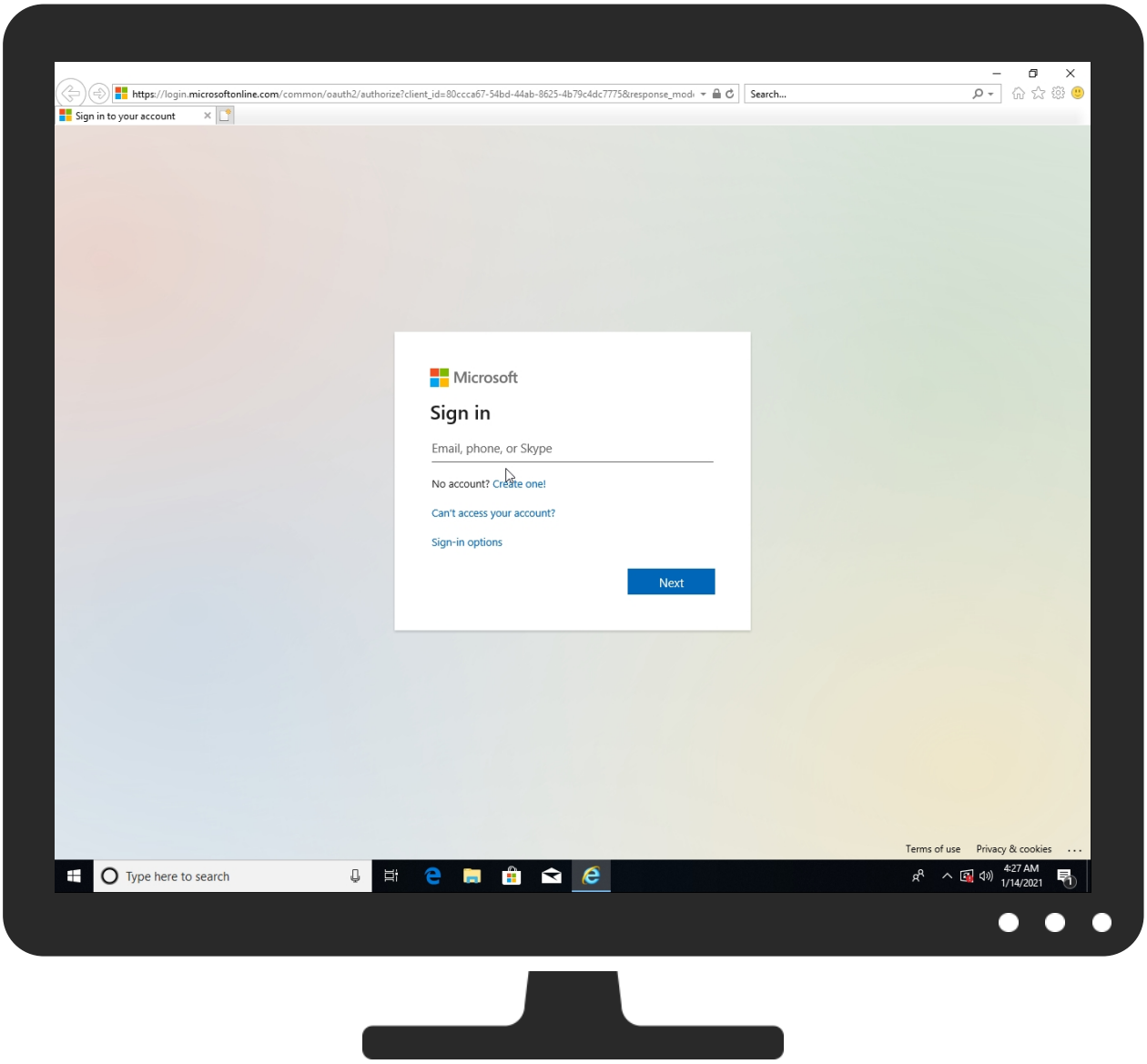


Screenshots

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
http://https://protection.office.com/campaigns	0%	Virustotal		Browse
http://https://protection.office.com/campaigns	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cs1100.wpc.omegacdn.net	0%	Virustotal		Browse
sni1gl.wpc.alphacdn.net	0%	Virustotal		Browse
aadcdn.msftauth.net	0%	Virustotal		Browse
assets.onestore.ms	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://aadcdn.msftauth.net/shared/1.0/content/js/ConvergedLogin_PCore_jwYGVbAxVLRxtzxSQp7jCQ2.js	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net	0%	URL Reputation	safe	
http://https://signup.live.cotonline.com/common/oauth2/authorize?client_id=80ccca67-54bd-44ab-8625-4b79c4dc	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~(	0%	Avira URL Cloud	safe	
http://https://www.youradchoices.ca/fr	0%	URL Reputation	safe	
http://https://www.youradchoices.ca/fr	0%	URL Reputation	safe	
http://https://www.youradchoices.ca/fr	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/lwsignupstringscountrybirthdate_en-us_pVtahKS9WUIZdNqg1DDhHg2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/lwsignupstringscountrybirthdate_en-us_pVtahKS9WUIZdNqg1DDhHg2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/lwsignupstringscountrybirthdate_en-us_pVtahKS9WUIZdNqg1DDhHg2.js?v=1	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~	0%	Avira URL Cloud	safe	
http://https://privacy.micros	0%	URL Reputation	safe	
http://https://privacy.micros	0%	URL Reputation	safe	
http://https://privacy.micros	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2.js?v=1	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	Avira URL Cloud	safe	
http://https://www.youradchoices.ca	0%	URL Reputation	safe	
http://https://www.youradchoices.ca	0%	URL Reputation	safe	
http://https://www.youradchoices.ca	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/lightweightsignuppackage_mStdClDku7grp_TX7Xaf-g2.js?v=1	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/images/microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2.svg	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2.svg	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2.svg	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/favicon.ico?v=2~	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/favicon.ico?v=2~	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/favicon.ico?v=2~	0%	URL Reputation	safe	
http://www.mpegla.com).	0%	Avira URL Cloud	safe	
http://https://signup.live.co	0%	URL Reputation	safe	
http://https://signup.live.co	0%	URL Reputation	safe	
http://https://signup.live.co	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	0%	URL Reputation	safe	
http://https://www.skype.com).	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/images/favicon.ico?v=2~(	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/favicon.ico?v=2~(	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/favicon.ico?v=2~(	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/converged_ux_v2_RfnRCrmapm3W_OFn994CMA2.css?v=1	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/ux.converged.login.strings-en.min_xw0hy9kams	0%	Avira URL Cloud	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/2_vD0yppaJX3jBnfbHF1hqXQ2.svg)	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/2_vD0yppaJX3jBnfbHF1hqXQ2.svg)	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/2_vD0yppaJX3jBnfbHF1hqXQ2.svg)	0%	URL Reputation	safe	
http://https://www.microsoft.	0%	URL Reputation	safe	
http://https://www.microsoft.	0%	URL Reputation	safe	
http://https://www.microsoft.	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/favicon.ico?v=2	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/favicon.ico?v=2	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/favicon.ico?v=2	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cs1100.wpc.omegacdn.net	152.199.23.37	true	false	• 0%, Virustotal, Browse	unknown
sni1gl.wpc.alphacdn.net	152.199.21.175	true	false	• 0%, Virustotal, Browse	unknown
signup.live.com	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
protection.office.com	unknown	unknown	false		high
login.microsoftonline.com	unknown	unknown	false		high
assets.onestore.ms	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
acctcdn.msauth.net	unknown	unknown	false		unknown
ajax.aspnetcdn.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://login.microsoftonline.com/common/oauth2/authorize?client_id=80ccca67-54bd-44ab-8625-4b79c4dc7775&response_mode=form_post&response_type=code+id_token&scope=openid+profile&state=OpenIdConnect.AuthenticationProperties%3dRCxX7zvMbgWHQ4hQQjYDLsACHPdw0yPUh7ngOL7Hk3JPp31-2t6R1T1fqrzR8Ny3_NeRjSYengTKT4w7A0Dbye3ml6DtjwZfSs_SwfjQXQ-NW757XQkrsm6VSk6fhaKscaKO6pM8w1lpm5_ei4_ovg&nonce=637461916115176785.YzM1MjNkNzgtZDgwNy00MDFkLThlMzktMDFjMjZmODEwMzA1MTFhNWM1MTQtMzMyMi00NDJjLTllZWItZDQyYzc0ZTQ0NzBj&redirect_uri=https%3a%2f%2fprotection.office.com%2fcampaigns	false		high

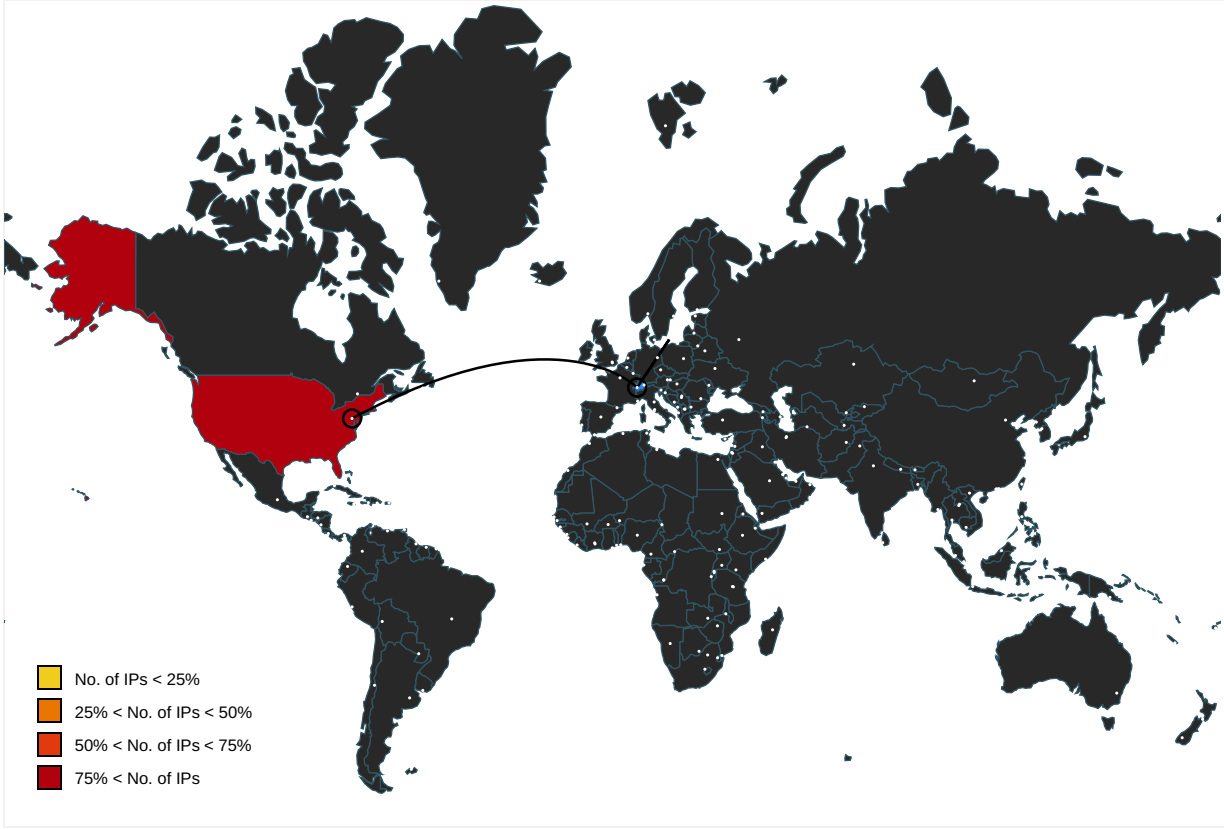
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aka.ms/useterms	servicesagreement[1].htm.2.dr	false		high
http://https://aka.ms/redeemrewards	servicesagreement[1].htm.2.dr	false		high
http://https://login.microsoftonline.com/	TokenBrokerCookies.exe, 00000006.00000002.652436055.0000016596410000.00000004.00000020.sdmp, TokenBrokerCookies.exe, 00000006.00000002.652451647.000001659641E000.00000004.00000020.sdmp, {567D1A1C-5618-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false		high
http://https://signin.kissmetrics.com/privacy/#controls	privacystatement[1].htm.2.dr	false		high
http://https://login.skype.com/login	privacystatement[1].htm.2.dr	false		high
http://https://www.acuityads.com/opt-out/	privacystatement[1].htm.2.dr	false		high
http://https://www.skype.com/go/ustax	servicesagreement[1].htm.2.dr	false		high
http://jquery.org/license	jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2[1].js.2.dr	false		high
http://https://aadcdn.msftauth.net/shared/1.0/content/js/ConvergedLogin_PCore_jwYGVbAxVLRxtzxSQp7jCQ2.js	authorize[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://acctcdn.msauth.net	signup[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://signup.live.cotonline.com/common/oauth2/authorize?client_id=80ccca67-54bd-44ab-8625-4b79c4dc	{567D1A1C-5618-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~(	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.optimizely.com/legal/opt-out/	privacystatement[1].htm.2.dr	false		high
http://sizzlejs.com/	jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2[1].js.2.dr	false		high
http://https://www.youradchoices.ca/fr	privacystatement[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://acctcdn.msauth.net/lwsignupstringscountrybirthdate_en-us_pVtahKS9WUIZdNqg1DDhHg2.js?v=1	signup[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.adr.org	servicesagreement[1].htm.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.xbox.com/en-US/Legal/CodeOfConduct)	servicesagreement[1].htm.2.dr	false		high
http://www.asp.net/ajaxlibrary/CDN.ashx.	privacystatement[1].htm.2.dr	false		high
http://https://signup.live.com/error.aspx?errcode=1045&mkt=en-US	signup[1].htm.2.dr	false		high
http://https://login.windows-ppe.net	Me[1].htm.2.dr	false		high
http://https://www.xbox.com/en-US/Legal/CodeOfConduct	servicesagreement[1].htm.2.dr	false		high
http://opensource.org/licenses/mit-license.php)	knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2[1].js.2.dr	false		high
http://www.json.org/json2.js	knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2[1].js.2.dr	false		high
http://https://aka.ms/taxservice	servicesagreement[1].htm.2.dr	false		high
http://https://www.privacyshield.gov/welcome	privacystatement[1].htm.2.dr	false		high
http://https://login.microsoftonline.com	Me[1].htm.2.dr	false		high
http://https://ondemand.webtrends.com/support/optout.asp	privacystatement[1].htm.2.dr	false		high
http://https://www.skype.com/go/legal.broadcast	servicesagreement[1].htm.2.dr	false		high
http://https://aadcdn.msftauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://skype.com/go/myaccount	servicesagreement[1].htm.2.dr	false		high
http://https://www.skype.com	servicesagreement[1].htm.2.dr	false		high
http://https://www.appsflyer.com/optout	privacystatement[1].htm.2.dr	false		high
http://https://privacy.micros	{567D1A1C-5618-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.appnexus.com/	privacystatement[1].htm.2.dr	false		high
http://https://acctcdn.msauth.net/knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2.js?v=1	signup[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://aka.ms/redeemrewards).	servicesagreement[1].htm.2.dr	false		high
http://https://login.microsoftonline.com/jsdisabled	authorize[1].htm.2.dr	false		high
http://https://aadcdn.msftauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	imagestore.dat.2.dr, authorize[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.mpegla.com	servicesagreement[1].htm.2.dr	false		high
http://https://www.youradchoices.ca	privacystatement[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://priv-policy.imrworldwide.com/priv/browser/us/en/optout.html	privacystatement[1].htm.2.dr	false		high
http://github.com/requirejs/almond/LICENSE	50-f1e180[1].js.2.dr	false		high
http://https://www.youronlinechoices.com/	privacystatement[1].htm.2.dr	false		high
http://https://mixer.com/contact	servicesagreement[1].htm.2.dr	false		high
http://https://www.here.com/)	privacystatement[1].htm.2.dr	false		high
http://https://www.skype.com/go/store.reactivate.credit	servicesagreement[1].htm.2.dr	false		high
http://https://acctcdn.msauth.net/lightweightsignuppackage_mStdCIDku7grp_TX7Xaf-g2.js?v=1	signup[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.aboutads.info/	privacystatement[1].htm.2.dr	false		high
http://https://www.adjust.com/opt-out/	privacystatement[1].htm.2.dr	false		high
http://https://www.xbox.com/managedatacollection	privacystatement[1].htm.2.dr	false		high
http://https://signup.live.com/	{567D1A1C-5618-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false		high
http://https://www.xbox.com/xbox-game-studios)	servicesagreement[1].htm.2.dr	false		high
http://https://acctcdn.msauth.net/images/microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2.svg	signup[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://acctcdn.msauth.net/images/favicon.ico?v=2~	imagestore.dat.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://developer.yahoo.com/flurry/end-user-opt-out/	privacystatement[1].htm.2.dr	false		high
http://fontello.com	icons[1].eot.2.dr	false		high
http://www.mpegla.com).	servicesagreement[1].htm.2.dr	false	• Avira URL Cloud: safe	low
http://https://signup.live.co	{567D1A1C-5618-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	signup[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.skype.com).	servicesagreement[1].htm.2.dr	false	• Avira URL Cloud: safe	low
http://https://www.xbox.com	privacystatement[1].htm.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://knockoutjs.com/	knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2[1].js.2.dr, Converged Login_PCore_jwYGVbAxVLRxtzxSQp7jCQ2[1].js.2.dr	false		high
http://https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protectio	privacystatement[1].htm.2.dr	false		high
http://https://github.com/douglascrockford/JSON-js	ConvergedLogin_PCore_jwYGVbAxVLRxtzxSQp7jCQ2[1].js.2.dr, signup[1].htm.2.dr	false		high
http://https://www.clicktale.net/disable.html	privacystatement[1].htm.2.dr	false		high
http://https://acctcdn.msauth.net/images/favicon.ico?v=2~(	imagestore.dat.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.skype.com/go/allrates	servicesagreement[1].htm.2.dr	false		high
http://https://acctcdn.msauth.net/converged_ux_v2_RfnRCrmapm3W_OFn994CMA2.css?v=1	signup[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.opensource.org/licenses/mit-license.php)	knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2[1].js.2.dr	false		high
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/ux.converged.login.strings-en.min_xw0hy9kams	authorize[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.xbox.com/xbox-game-studios	servicesagreement[1].htm.2.dr	false		high
http://fontello.comiconsRegulariconsiconsVersion	icons[1].eot.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://acctcdn.msauth.net/images/2_vD0yppaJX3jBnfbHF1hqXQ2.svg)	signup[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html	privacystatement[1].htm.2.dr	false		high
http://https://www.skype.com/go/legal	servicesagreement[1].htm.2.dr	false		high
http://https://mixer.com/about/tos	servicesagreement[1].htm.2.dr	false		high
http://https://www.microsoft.	{567D1A1C-5618-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://acctcdn.msauth.net/images/favicon.ico?v=2	imagestore.dat.2.dr, signup[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://aadcdn.msftauth.net	authorize[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.xbox.com/	privacystatement[1].htm.2.dr	false		high
http://https://github.com/h5bp/html5-boilerplate/blob/master/src/css/main.css	app[1].css.2.dr	false		high
http://https://www.linkedin.com/legal/privacy-policy	privacystatement[1].htm.2.dr	false		high
http://https://login.microsoftonline.com/common/oauth2/authorize?client_id=80ccca67-54bd-44ab-8625-4b79c4dc	~DFB66D0A2BAC6D7BF1.TMP.1.dr	false		high
http://https://login.microsoftonline.com/0tbauth://login.windows.net/?context=https%3A%2F%2Flogin.microsoft	TokenBrokerCookies.exe, 00000006.00000002.652444483.0000016596418000.00000004.00000020.sdmp	false		high
http://jquery.com/	jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2[1].js.2.dr	false		high
http://https://support.xbox.com/help/friends-social-activity/community/use-safety-settings	privacystatement[1].htm.2.dr	false		high
http://https://www.xbox.com/Legal/ThirdPartyDataSharing	privacystatement[1].htm.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
152.199.21.175	unknown	United States		15133	EDGECASTUS	false
152.199.23.37	unknown	United States		15133	EDGECASTUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339453
Start date:	14.01.2021
Start time:	04:26:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://protection.office.com/campaigns
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:	17
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean2.win@5/59@8/2
EGA Information:	Failed

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://login.live.com/oauth20_authorize.srf?response_type=code&client_id=51483342-085c-4d86-bf88-cf50c7252078&scope=openid+profile+email+offline_access&response_mode=form_post&redirect_uri=https%3a%2f%2flogin.microsoftonline.com%2fcommon%2ffederation%2foauth2&state=rQIIAY1SPW_TUBS1mzZtI6AVYmDsgIQEcvJeYvslkTqkMVWaxE6cuCTxEjmOvz-xjd14YYQFUTF2hK0SA7AgJCQktk6dKzYGUCfKBBIDbn8By9WR7jlX99xz7-VgEdbvVIEsyxKNCIqczQmSlGZElS5TBDlDNZmcywghKrhZ2Lw4x87err7ffb2y8eT5S7F3hK9PbSNWirLnHON39Sjyw3qp5AdepMiR4blFT1UN-apfkiXHlwzNDT_g-CmO_8Dx46WQriCShjVIQ0hBRKMqVZykLGRNzuJSLRIZLeEWALDMrtUVdJtNrSjDJmuKTo95kLBpA7LCrs6NMo3AR2zKLlgDAI5pm13BtsXRXjaDX0xSGYgCD7h0xzxb2ug1Hkd6-bJ4gZEqv5bWVS9wpr4XRke5T3jPV9y9edNz3cxF8ZKmuJEhS5eO-oHnK0FkKOH2oHkwRmnMzrRRiyd1njcnTDdsNFv9eQIW_X0duVqvi1pWpd33K5AoR_QAClB9FKSDKreoTDllYA4niqsJHYFMUAMws4VScWyaicxEVlfhdJioJj_mCW6EKDTmrSB06ldDi1Z1qRPKUqdH-2w1gbbvUFPFIKderL3L5bNrO557kruRreoa860sD9WwldNl_Hz5GsjV19YKm9htbAv7vYy_Wsly_f41_lb7e9h8-uXFmz8XBexkpaTvDO6PawedThCjkjppW_tzEDMU3Y67Tq2rtdumVAVUi-17_DZdh4d5_DCf_5nHn61iH9f_9xPOCrfKoAwJAAllboFKvUzXKSh-vo79Aw2&estsfed=1&uaid=da00eaf107b146b3a3050f7f8d925a4f&signup=1&lw=1&fl=easi2&fci=80ccca67-54bd-44ab-8625-4b79c4dc7775 • Browsing link: https://www.microsoft.com/en-US/servicesagreement/ • Browsing link: https://privacy.microsoft.com/en-US/privacystatement

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, RuntimeBroker.exe, backgroundTaskHost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.43.139.144, 88.221.62.148, 52.109.88.132, 40.126.1.130, 20.190.129.24, 20.190.129.2, 40.126.1.166, 20.190.129.133, 40.126.1.128, 20.190.129.17, 20.190.129.128, 20.190.129.130, 20.190.129.19, 40.126.1.142, 20.190.129.160, 51.104.139.180, 13.107.42.22, 52.114.128.43, 92.122.213.194, 92.122.213.247, 92.122.145.53, 92.122.213.200, 92.122.213.219, 13.107.246.13, 152.199.19.160, 2.20.85.93, 152.199.19.161, 92.122.213.240, 84.53.167.109, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, assets.onestore.ms.edgekey.net, www.tm.lg.prod.aadmsa.akadns.net, e13678.dscb.akamaiedge.net, browser.events.data.trafficmanager.net, i.s-microsoft.com.edgekey.net, www.tm.a.prd.aadg.trafficmanager.net, a1945.g2.akamai.net, e11290.dspg.akamaiedge.net, www.microsoft.com-c-3.edgekey.net, login.live.com, star-azurefd-prod.trafficmanager.net, statics-marketingsites-eus-ms-com.akamaized.net, watson.telemetry.microsoft.com, acctcdnvzeuno.azureedge.net, a1778.g2.akamai.net, acctcdnvzeuno.ec.azureedge.net, standard.t-0003.t-msedge.net, e10583.dspg.akamaiedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, aadcdnoriginneu.azureedge.net, skypedataprdcolcus16.cloudapp.net, www.tm.a.prd.aadg.akadns.net, statics-marketingsites-wcus-ms-com.akamaized.net, assets.onestore.ms.akadns.net, c-s.cms.ms.akadns.net, t-0003.t-msedge.net, dub2.current.a.prd.aadg.trafficmanager.net, blobcollector.events.data.trafficmanager.net, account.msa.akadns6.net, c.s-microsoft.com-c.edgekey.net, privacy.microsoft.com.edgekey.net, cs9.wpc.v0cdn.net, protection.office.trafficmanager.net, i.s-microsoft.com, a1449.dscg2.akamai.net, arc.msn.com, acctcdn.trafficmanager.net, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, go.microsoft.com, mscomajax.vo.msecnd.net, skypedataprdcolcus04.cloudapp.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, cs22.wpc.v0cdn.net, ie9comview.vo.msecnd.net, protectioncenterweuprod.cloudapp.net, Edge-Prod-FRAr3.ctrl.t-0003.t-msedge.net, login.msa.msidentity.com, aadcdnoriginneu.ec.azureedge.net, skypedataprdcoleus17.cloudapp.net, browser.events.data.microsoft.com, c.s-microsoft.com, privacy.microsoft.com, go.microsoft.com.edgekey.net, l-0013.l-msedge.net, e13678.dscg.akamaiedge.net, www.microsoft.com, e13678.dspb.akamaiedge.net, wcpstatic.microsoft.com • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{567D1A1A-5618-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8472959958577402
Encrypted:	false
SSDEEP:	192:raZFZA2q9WttQif6vhzMVVepBVV9jDVVOsfVVevMjX:rGrXqUXdn8t1z
MD5:	3936AFF65D34369B7290F7512981A844
SHA1:	46BFB03F39C413ECA699213B232E9D294BA79C13
SHA-256:	37954BC180971B56B19CC9CF57B04540A7191F80402D3E7598ACE95872358F94
SHA-512:	0E79572E7805DE1199E7FEC163D273265C16B6B3FB7E80CAB9F0336D9F2C64F1E195FE5E526C7E53DB65B0CC5047AB915FFEB747A84FF8569795935563CBB473
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{567D1A1C-5618-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	105980
Entropy (8bit):	3.3243761032424533
Encrypted:	false
SSDEEP:	1536:ISgu0ApBLHgu00pBLqpBLUpBL9pBLbpBL9pBLXpBLrpBLJ:IPakec+hXhznJ
MD5:	9D64BE0DCE95D92CEC45EC74B1A9CCCD
SHA1:	87C826887B12B00780CCECDC234B753476A97303
SHA-256:	D7B8A7C38591C0EE6749B092CDEC5071CF6FC536EB14C174F5E45F603B722AC9
SHA-512:	57D4A828C37120EDA7397BC4CA14847A9F78183B5FB7E1E475A3CAE13AD944CA3049F7B00C2B7416D899D216CD143F60C40070984120D45E919E9AD12F2DE0D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{567D1A1C-5618-11EB-90EB-ECF4BBEA1588}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{567D1A1D-5618-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5657697473971386
Encrypted:	false
SSDEEP:	48:IwfGcpr+GwpanG4pQ7jGrapbSMrGQpKpQG7HpRDsTGIpG:r1Z2QJ6DBSMFA9TD4A
MD5:	A6377BE99E639130AEF14785146C1E77
SHA1:	D579DB4FCEF199C6C1A2EA8EC8F9900E90639C11
SHA-256:	9EF8ADF1B7A9B673FC6879A493E062F09065DAADB92A59E688148F2BB267A79F
SHA-512:	90C1780145BFD666794143DB7108439DB88FDF687772244AE835FEFC0DE4A2C6CB54FA32821E965E04CC4B46F1793C1E2DCB0A0881744676D3E80DB7B275A40I
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	72332
Entropy (8bit):	3.0749533542606953
Encrypted:	false
SSDEEP:	96:NMLMiMiMDM6M9QQQQQsQQQQQgQQQQQgQQQQQN:NGPv6HZ
MD5:	2831458E3A3CFD909DAA46E907FB5D2D
SHA1:	34C7A4232301D8CB28251600ED9E168150CBA0E9
SHA-256:	756E74113F78025BAF5E8CC7A0995C0E2897B93A3C5533F735789C8139BFC40F
SHA-512:	334CAACF1DEBCB5EC9978E5B6AAEF15427A8490CC4FEB64F671D01ED17289262BB362F97ED51993F20C3697CD0CB1FD942493AA073D0F0B2BABFA0228FFB4D CF
Malicious:	false
Reputation:	low
Preview:	[.h.t.t.p.s.:./.a.a.d.c.d.n...m.s.f.t.a.u.t.h...n.e.t./.s.h.a.r.e.d./.1...0./.c.o.n.t.e.n.t./.i.m.a.g.e.s./.f.a.v.i.c.o.n._.a._.e.u.p.a.y.f.g.g.h.q.i.a.i.7.k.9.s.o.l.6.l.g.2...i.c.o.~(.....h(..... (.....(.....".P..... 333333333

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\2_bc3d32a696895f78c19df6c717586a5d[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1864
Entropy (8bit):	5.222032823730197
Encrypted:	false
SSDEEP:	48:yvswNIBLBpJawmMH44log6gw/MHm7pJroog6gwkMH9Xog6gwdMHdqdyqog7C:ykfXYx+odPcs9B
MD5:	BC3D32A696895F78C19DF6C717586A5D
SHA1:	9191CB156A30A3ED79C44C0A16C95159E8FF689D
SHA-256:	0E88B6FCBB8591EDFD28184FA70A04B6DD3AF8A14367C628EDD7CABA32E58C68
SHA-512:	8D4F38907F3423A86D90575772B292680F7970527D2090FC005F9B096CC81D3F279D59AD76EAFCA30C3D4BBAF2276BBAA753E2A46A149424CF6F1C319DED5A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/shared/1.0/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\2_bc3d32a696895f78c19df6c717586a5d[1].svg	
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6z" fill="url(#A)"/><path d="M394.2 1815.6c746.58 0 1351.8-493.2 1351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 1815.6 394.2 1815.6z" fill="url(#B)"/><path d="M1548.6 1885.2c631.92 0 1144.2-417.45 1144.2-932.4S2180.52 20.4 1548.6 20.4 404.4 437.85 404.4 952.8s512.276 932.4 1144.2 932.4z" fill="url(#C)"/><path d="M265.8 1215.6c690.246 0 1249.8-455.595 1249.8-1017.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUnits="userSpaceOnUse" gradientTransform="translate(1466.4 393.6) rotate(90) scale(1401.6 1720.8)"><stop stop-color="#107c10"/><stop offset="1" stop-color="#c4c4c4" stop-opacity="0"/></radialGradient><r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ConvergedLogin_PCore_jwYGVbAxVLRxtzxSQp7jCQ2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	429236
Entropy (8bit):	5.430242833372782
Encrypted:	false
SSDEEP:	6144:iR7UuYFUhMXrYqbIkB4D9DZX/M623WkYcYyOCtPE0HKRVpA:U7M5XCkB4h5tSyu
MD5:	8F060655B03154B471B73C52429EE309
SHA1:	03E3585E81FBC4996877F3AF5C25AB2DFF30AD56
SHA-256:	8D4C8938578F6ADB95A07665C4C092625B34B273B10F960D343311552E958E2B
SHA-512:	AD0DC65C47755BD1DDAE4B1BA5842B989939AB3D1B5DC9D204BF0F29178CF521E2CF2A436F16CE693DC0E005387FB6CB719A2ABF08D18182400C9224070362 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/shared/1.0/content/js/ConvergedLogin_PCore_jwYGVbAxVLRxtzxSQp7jCQ2.js
Preview:	/*!. * ---------- START OF THIRD PARTY NOTICE ----------. * . * This file is based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise.. * . * json2.js (2016-05-01). * https://github.com/douglascrockford/JSON-js. * License: Public Domain. * . * Provided for Informational Purposes Only. * . * ---------- END OF THIRD PARTY NOTICE ----------. */!function(e){function n(n){for(var t,i,o=n[0],r=n[1],s=0,c=[];s<o.length;s++)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\arrow_px_up[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 7 x 9
Category:	downloaded
Size (bytes):	829
Entropy (8bit):	0.6055646407132698
Encrypted:	false
SSDEEP:	3:CKY1q/rylAxrt/laIFBYEQvyIFle:sGFaIFBYfvDfe
MD5:	95B65C94F57061E15ECC8304D3E578D5
SHA1:	A7483D668A780949FDA842F39877A3C08D0FC51C
SHA-256:	BDA2D6EB8E72B3DBCA5EEF086178033F8A2BB3481180B2C63295FCF23843D960
SHA-512:	B17552D90D0038531A5F4E78DA553F9109346CB25851F38996BFAB54906A898DE848FEFFD31E8D0BF0A32D956513CA7ED72D2F4C3AE47922C6F9D370584288EF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/arrow_px_up.gif?version=27f11222-771f-bb95-a744-f0b962f89b91
Preview:	GIF89a.....3..... ....!.....,..... ..... .`.....\8....!>L(.b@.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\authorize[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):	188804
Entropy (8bit):	5.646492052117407
Encrypted:	false
SSDEEP:	3072:x83WX+BjEJ4yVUS5kdTG2ym+d/PngTehliy2g/q+Y:Iy+qkdTGzBY
MD5:	8AEC44FC117228C47FA14C6F0298707E
SHA1:	0E6AE678E174E3A67E71280ED0EC1C1542DE5EB8
SHA-256:	10ED783181B49A61234E0851CCD23647E97E6EEFAA7EF00ED103C5E7F9913838
SHA-512:	A8F44D5AC7765D29785D362CD5FE74E92BE0227BA99AFDF632D4BEF8EB2538928F1AAB338B2338C7D21D6BB861C62496A26B07DB2AD71BDC5B491E927F7C5C F7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\authorize[1].htm	
Preview:	.... Copyright (C) Microsoft Corporation. All rights reserved. -->..<!DOCTYPE html>..<html dir="ltr" class="" lang="en">..<head>.. <title>Sign in to your account</title>.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <meta http-equiv="X-UA-Compatible" content="IE=edge">.. <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=2.0, user-scalable=yes">.. <meta http-equiv="Pragma" content="no-cache">.. <meta http-equiv="Expires" content="-1">.. <link rel="preconnect" href="https://aadcdn.msftauth.net" crossorigin>..<meta http-equiv="x-dns-prefetch-control" content="on">..<link rel="dns-prefetch" href="//aadcdn.msftauth.net">..<link rel="dns-prefetch" href="//aadcdn.msauth.net">.... <meta name="PageID" content="ConvergedSignIn" />.. <meta name="SiteID" content="" />.. <meta name="ReqLC" content="1033" />.. <meta name="LocLC" content="en-US" />.... <meta name="referrer" content="origin" />....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cf-7c36ab[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):	168646
Entropy (8bit):	5.044051581582224
Encrypted:	false
SSDEEP:	3072:OzCPZkTP3bDLH0tfRqQ0xtLfj4ZDSIpTt813viY8R1j35Ap7LQZLPPJH7PAbOCxR:clZAXLkeedh
MD5:	0DCFF2779D4542C11AD9C9C19DF8328D
SHA1:	D7EFAE8E66FA6B4C335826BFD8C56C6F142E4254
SHA-256:	440D8292ABDF80DD6E8A9D9FAEA83367CE57BD1A1A8D153EDC358DB5F97EFF35
SHA-512:	CC747AA36ADEE4CBA4236F01820CE9661214C649DCF23227D7CF9187E24F2D15DBA43E9B706B30DC3D55060E08601575EAB0256306AEA28F3544BAD4BC33E9 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-eus-prod/west-european/shell/_scrf/css/themes=default.device=uplevel_web_pc/93-de417f/39-6894a8/60-0f9daa/9c-879d19/5f-d422a2/ea-c61049/a7-5072ba/cf-7c36ab?ver=2.0
Preview:	@charset "UTF-8";./*! | 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 */.body{margin:0}.context-uh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\converged_ux_v2_RfnRCrmapm3W_OFn994CMA2[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	95459
Entropy (8bit):	5.292153801820765
Encrypted:	false
SSDEEP:	1536:QpHDIqBBw+T6azA/PWrF7qvEAFiQcpmKboBdiyMUWC8ErpH/TVTDrwCGNJZ3yU0P:IBFNyUM
MD5:	45F9D10AB99AA66DD6FCE167F7DE0230
SHA1:	D443993E7ADB3108167BCD94E5D3126A2E3EE7EE
SHA-256:	D72952FC8950D26C08C6BAD73D389C35D0EAF164CB73503183A2966DEFAAD991
SHA-512:	0DBCCCB37A3A249C7DBB948AC756FD332298DD8A742E92DF6A767FD565C925768058C05AF182106F8DA29979C0D23BD3E9ECE9E41C1EA931F4F198CBDCE8B 3F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/converged_ux_v2_RfnRCrmapm3W_OFn994CMA2.css?v=1
Preview:	/*! Copyright (C) Microsoft Corporation. All rights reserved. *//*!---------- START OF THIRD PARTY NOTICE ----------..This file based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise. .//----------.twbs-bootstrap-sass (3.3.0).//----------..The MIT License (MIT)..Copyright (c) 2013 Twitter, Inc..Permission is hereby granted, free of charge, to any perso

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jquery-1.7.2.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	94840
Entropy (8bit):	5.372946098601679
Encrypted:	false
SSDEEP:	1536:8YRKUfAjtledhTmtaFyQHGvCXsedOgRc9izzr4yff8teLvHHEjam7W5X3yzSiLnM:VUb6GvCu09s2o2skAieW
MD5:	B8D64D0BC142B3F670CC0611B0AEBCAE
SHA1:	ABCD2BA13348F178B17141B445BC99F1917D47AF
SHA-256:	47B68DCE8CB6805AD5B3EA4D27AF92A241F4E29A5C12A274C852E4346A0500B4
SHA-512:	A684ABBE37E8047C55C394366B012CC9AE5D682D29D340BC48A37BE1A549AECED72DE6408BEDFED776A14611E6F3374015B236FBF49422B2982EF18125FF47D C
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jquery-1.7.2.min[1].js	
Reputation:	low
IE Cache URL:	http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.7.2.min.js
Preview:	/*! jQuery v1.7.2 jquery.com | jquery.org/license */.(function(a,b){function cy(a){return f.isWindow(a)?a:a.nodeType===9?a.defaultView||a.parentWindow:!1}function cu(a){if(!cj[a]){var b=c.body,d=f("<"+a+">").appendTo(b),e=d.css("display");d.remove();if(e==="none"||e===""){ck||(ck=c.createElement("iframe"),ck.frameBorder=ck.width=ck.height=0),b.appendChild(ck);if(!cl||!ck.createElement)cl=(ck.contentWindow||ck.contentDocument).document,cl.write((f.support.boxModel?"<!doctype html>":"")+"<html><body>"),cl.close();d=cl.createElement(a),cl.body.appendChild(d),e=f.css(d,"display"),b.removeChild(ck)}cj[a]=e}return cj[a]}function ct(a,b){var c={};f.each(cp.concat.apply([],cp.slice(0,b)),function(){c[this]=a});return c}function cs(){cq=b}function cr(){setTimeout(cs,0);return cq=f.now()}function ci(){try{return new a.ActiveXObject("Microsoft.XMLHTTP")}catch(b){}}function ch(){try{return new a.XMLHttpRequest}catch(b){}}function cb(a,c){a.dataFilter&&(c=a.dataFilter(c,a.dataType));var d=a.dataTyp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2[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):	96649
Entropy (8bit):	5.297804550899051
Encrypted:	false
SSDEEP:	1536:G+6LPOpumEEni7iU2e25CxgjDb60nkN8h1utK0Dv+9G1LDrjsNyw5yn/dFZ75Tym:xH7pDuVUNB0lmEGWf
MD5:	E55ECB02E7376CD010C764107EBD513F
SHA1:	FA6D184DF01EC535628DC8FAF38211591BAADFC8
SHA-256:	5776881753B95A0ABE5D1F6EFE3ABE7B83A3265EACCD117DD948E523C044600C
SHA-512:	099C665E1CEE8DF9C5D5C340A14170341BD29E0321875FF08E594B750CFDBF2CA8C9B45B584FCA21F87CBE6CD8A170918CECFF8C9796AAFA3D89F0AA97509ABD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1
Preview:	/*!. * jQuery JavaScript Library v1.10.2. * http://jquery.com/. *. * Includes Sizzle.js. * http://sizzlejs.com/. *. * Copyright 2005, 2013 jQuery Foundation, Inc. and other contributors. * Released under the MIT license. * http://jquery.org/license. *. * Date: 2013-07-03T13:48Z. */.!function(e,t){function n(e){var t=e.length,n=ct.type(e);return ct.isWindow(e)?!1:1===e.nodeType&&t?!0:"array"===n||"function"!==n&&(0===t||"number"==typeof t&&t>0&&t-1 in e)}function r(e){var t=kt[e]={};return ct.each(e.match(pt)||[],function(e,n){t[n]=!0}),t}function i(e,n,r,i){if(ct.acceptData(e)){var o,a,s=ct.expando,u=e.nodeType,l=u?ct.cache:e,c=u?e[s]:e[s]&&s;if(c&&l[c]&&(i||l[c].data)||r!==t||"string"!=typeof n){return c||(c=u?e[s]=tt.pop()||ct.guid++:s),l[c]||(l[c]=u?{}:{"toJSON":ct.noop}),("object"==typeof n||"function"==typeof n)&&(i?l[c]=ct.extend(l[c],n):l[c].data=ct.extend(l[c].data,n)),a=l[c],i||(a.data||(a.data={}),a=a.data),r!==t&&(a[ct.camelCase(n)]=r),"string"==typeof n?(o=a[n],null==o&&(o=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\lwsignupstringscountrybirthdate_en-us_pVtahKS9WUIZdNqg1DDhHg2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	26214
Entropy (8bit):	5.070912570595838
Encrypted:	false
SSDEEP:	384:Z3EReHg2sQhdCdfqPxZebPrmuex3dmac3zirs7rOubUrUA/4RkD:lQAg2sQ8q2bPrmjx3dmac3ziarbnA1
MD5:	A55B5A84A4BD59421974DAA0D430E11E
SHA1:	09926A2D8BBFA41C3085BCF8A546AEAD3FB8C0FC
SHA-256:	FC6D389E166EBA3F121C4A92F446C1C36997D770862F4D6994192CE1AD4A1051
SHA-512:	80E302F28ABB96953E84EABB9D56106D8AA3C410A54A3185588BAA9709CDBF33752D263447814A55AEBE5E7E0BB14396B02732111906792059FE6D9A5F626AF5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/lwsignupstringscountrybirthdate_en-us_pVtahKS9WUIZdNqg1DDhHg2.js?v=1
Preview:	!function(){registerNamespace("$Config"),$Config.sharedStrings={"errors":{"required":"This information is required.","emailRequired":"An email address is required","phoneRequired":"A phone number is required","passwordRequired":"A password is required","invalidEmailFormat":"Enter the email address in the format someone@example.com.","invalidPhoneFormat":"The phone number you entered isn't valid. Your phone number can contain numbers, spaces, and these special characters: ( ) [ ] . - * /","emailMustStartWithLetter":"Your email address needs to start with a letter. Please try again.","memberNameAvailable":"{0} is available.","memberNameAvailableEasi":"After you sign up, we'll send you a message with a link to verify this user name.","memberNameExistsPhone":"If you own a Microsoft account with this number, go back and sign in.","proofAlreadyExistsError":"This is already part of your security info.","signupBlocked":"{0} isn't available.","memberNameTakenPhone":"The phone number you typed i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2[1].svg	
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/images/microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38 .119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392, 1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47. 081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0, 0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.61 1,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.9 52,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\print-icon[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	173
Entropy (8bit):	5.970149697517944
Encrypted:	false
SSDEEP:	3:yionv//thPl9vtt+NTl0qRthwkBDsTBZtqmA73Fs+rQx33npdtnoypZh9Dicl2up:6v/lhPmNp0WnDspBAzqPnpdiyTh9Fp
MD5:	023F5AC6E0114AF1F781BE5D3C956385
SHA1:	C166284B8541F1DE32DC5C4DEC635C296BF85C98
SHA-256:	75D637BF6B6DFF2525095D0BE7E0C90F012BB118C2EF19099AFDCBC630ADFC79
SHA-512:	DAFA49056E3D3014DB392410685CC05773C09938E2E700657727928EDCFF8EA2D7C769D377539C52DA70321B94F4E8F045F565EC51BC2B701D95BB3213CC2203
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/print-icon.png?version=60ebb5de-511c-db20-3795-563c739c5e12
Preview:	.PNG.....IHDR.....h6....tEXtSoftware.Adobe ImageReadyq.e<...OIDATx.b...?..0222`..jX..a5...D0.50.....k.....:...X=....'..(..I.....K..... .....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\script[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):	50466
Entropy (8bit):	5.403327253117392
Encrypted:	false
SSDEEP:	768:3Vs4A3c/bSKCzUm4D19h3j9UIAyjYXQgyjYXEoygRRsRnMtoafRnvdMIKebqH:h6c/bSKCzUm4DDh3j+9XQ4XE+BZdMIK9
MD5:	633B23CA8A850C508C146635DB4239F5
SHA1:	CF78DA53BD7561F3ACB33710016ECBF60E9F0204
SHA-256:	DAA1677D2640BE8A77F6C69EEE3911D2F8CF81DAA7BB604800A2D63A8F130C95
SHA-512:	82D4887AB9BB6A449FB0E5B6DEF80215B5F9E51058DCB1B8B7CD583A880F93428C3FB75B37C0E9481843203A4878FEF32424B5CD2EBCDD811D92604A1C1BCA B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=1a053411-4f63-d069-d3b8-11d5d720eeb4
Preview:	function ShowSelectedComponentKeyPress(n,t){if(window.event.keyCode==13)return ShowSelectedComponent(n,t),!1}function ShowHighLight(n){var t=$("#div"+ n).height();$.browser.msie&&parseInt($.browser.version,10)==7?$("#div"+n+" > .highlight").css({width:"0",height:"0","background-color":"white",float:"left","border-top":M ath.round(t/2+.3)+"px solid white","border-right":"0.75em solid "+$("#div"+n).css("background-color"),"border-bottom":Math.round(t/2+.3)+"px solid white"}):$("#div"+n+" > .highlight").css({width:"0",height:"0","background-color":"white",float:"left","border-top":t/2+.3+"px solid white","border-right":"0.75em solid "+$("#div"+n).css("background-color"),"border-bottom":t/2+.3+"px solid white"})}function SetRightSideNavigationMenuHeight(){$("[id^=dvModuleGroup_]").hide();window.location.search.toLowerCase(). indexOf("bookmarkid")!=-1&&SelectBookMark();window.location.search.toLowerCase().indexOf("componentid")!=-1&&LoadSelectedInternalLink();$(".div_side_comp").leng th>0&&$(".

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\script[2].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):	30173
Entropy (8bit):	5.326896118392395
Encrypted:	false
SSDEEP:	384:ekorlyUMfQ8sW5hXDiWiQRKKwoOdo/r4nqdRy/dRyWhtyFhtyYKQys05DU7BS5hN:0olDi2RKQOOwqjE2l/3FJ1C/nrjYiKq
MD5:	F620D4D38655075DF3268D640BF479BD
SHA1:	79BEBF5E6907D4CDD5764B9B9CF3A72932F9C343
SHA-256:	7E1377CD02DAFE245ED719FCA972C5E8CFDE30CBF3910D2795A922BB466D08C2
SHA-512:	1A8528BDEEECEB75766B8ACCD7B5DBFE7E45E72A3E52108D3F63C0667ABF1492FBAFDD6F80E9639339BE5EE5C1E4A7B7BCA635C6DBBBEC83044FBC842C37 FFCC

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\script[2].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=42ce545a-d075-ac8e-38d1-8d9b4eaa1c7e
Preview:	function ShowSelectedComponentKeyPress(n,t){if(window.event.keyCode==13)return ShowSelectedComponent(n,t),!1}function SetRightSideNavigationMenuHeight(){$("[id^=dvModuleGroup_]").hide();window.location.search.toLowerCase().indexOf("bookmarkid")!=-1&&SelectBookMark();window.location.search.toLowerCase().indexOf("componentid")!=-1&&LoadSelectedInternalLink();$(".div_side_comp").length>0&&$(".div_content").css("min-height",$(".div_side_comp").height()-27)}function ShowSelectedComponent(n,t){var i=$("#"+t).attr("data-parentModule");return i!=undefined&&i!=null&&($("[data-parentmodule="+i+"]").show(),$("#"+i+" [id$=_LongDescription]").length>0?(document.getElementById(i+"_LongDescription").style.display="block",document.getElementById(i+"_ShortDescription").style.display="none",ShowText($("#"+i+".learnMoreLabel"),"long")):ShowText($("#"+i+".learnMoreLabel"),"long"),DisplayTopNavigation(i)),$("html, body").animate({scrollTop:$("#"+t).offset().top-1},800),!1}function ShowToolTip(){var n,i,t;w

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\50-f1e180[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	133618
Entropy (8bit):	5.224613249025047
Encrypted:	false
SSDEEP:	3072:1f/HuFVppxvIeJ0i9d1EwgXA9JKi5DCE5n:1f/Hu/FIeRxn
MD5:	04053017246241626706F1AB465531F
SHA1:	1C034383716BCE493E28BFFF0DD2C27F049CC558
SHA-256:	A5DD3C05EFED81BBF60B618C070A7746F030147590EE0EDD74459AC4E53955FD
SHA-512:	9D81E61D3B0AED73F7A64D0344E432AEAAAB057655CFEB040348FA876693E618A434D63727F1E4AA1118276740C7102FD412637B46752665B78EB3C81A53915A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-wcus-prod/shell/_scrf/js/themes=default/54-af9f9f/c0-247156/de-099401/e1-a50eee/e7-954872/d8-97d509/f0-251fe2/46-be1318/77-04a268/11-240c7b/63-077520/a4-34de62/bb-d7480b/db-bc0148/dc-7e9864/6d-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/79-499886/7e-cda2d3/b2-7087f0/e5-08f1c0/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/50-f1e180?ver=2.0&iife=1
Preview:	(function(){/**. * @license almond 0.3.3 Copyright jQuery Foundation and other contributors.. * Released under MIT license, http://github.com/requirejs/almond/LICENSE. */.var requirejs,require,define,__extends;(function(n){function r(n,t){return w.call(n,t)}function s(n,t){var o,s,f,e,h,p,c,b,r,l,w,k,u=t&&t.split("/"),a=i.map,y=a&&a["*"]||{};if(n){for(n=n.split("/"),h=n.length-1,i.nodeIdCompat&&v.test(n[h])&&(n[h]=n[h].replace(v,"")),n[0].charAt(0)==="."&&u&&(k=u.slice(0,u.length-1),n=k.concat(n)),r=0;r<n.length;r++)if(w=n[r],w==="."")n.splice(r,1),r-=1;else if(w===".."){if(r===0||r===1&&n[2]===".."||n[r-1]===".")continue;else r>0&&(n.splice(r-1,2),r-=2);n=n.join("/")}if((u||y)&&a){for(o=n.split("/"),r=o.length;r>0;r-=1){if(s=o.slice(0,r).join("/"),u)for(l=u.length;l>0;l-=1)if(f=a[u.slice(0,l).join("/")],f&&(f=f[s],f)){e=f;p=r;break}if(e)break;!c&&y&&y[s]&&(c=y[s],b=r)}!e&&c&&(e=c,p=b);e&&(o.splice(0,p,e),n=o.join("/"))}return n}function y(t,i){return function(){var r=b.call(arguments,0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Print[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	476
Entropy (8bit):	7.35124642782842
Encrypted:	false
SSDEEP:	12:6v/78/8QCeKXzjl5V6VQTdwbtsxET1SDQi7N:sNfF6VYd6tf1SdN
MD5:	B8E8859FCD4E43D51233559C17A3C7BD
SHA1:	F0CA023F26A84761995FA0BF6935DE6A3B8AE6F8
SHA-256:	DC15A37B4015D0DECF639006E4F9002E742DDBFD7C669EC0AE469057F238B78D
SHA-512:	3605E4C4FE22E6E05553F89D34CFE8B3E5CA72FBDADCCD8B279835A0ECEFCD10B1BF2AD1ACCEEB168EE369E23A8AD205720FBF33A184188A7F23AEA7B0F22005
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Print.png?version=03620f3a-5d1e-5a73-a117-a2f71eee437d
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....IDAT8O.S;..A.....M6.4....@.47....^I..<."&..W..Y...Y.....m...E.<..$..n...j..kL&.....}.j.....)@.....r..Q....]. .+.w...f3.R)...2^...ddO.^..Ud.BE..*D..h...!.....h..p..t...9.....1.."tD.....y.h.AQ.{."...J.D.U....c.b.i.h.t:..$&q..J..n.+9.r..B..F...e..`<...oS....Z-.H....NG...Jl..D.Z..@!...s<....m.'Ll..vc.?..~..v.n.9.;.m.5..K.A .....z=../>...M....r9..~...*..go.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\datarequestpackage_h-_7C7UzwdefXJT9njDBTQ2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	8111
Entropy (8bit):	5.339313763115951
Encrypted:	false
SSDEEP:	192:nEAKv577D9kgT/xwj9O8hFNFxgLdQ0Eoxr:E177Dj+yt
MD5:	87EFFB0BB533C1D79F5C94FD9E30C14D
SHA1:	4E4F5F3CDDDDBFDDB46A1626D7CE579A639DE389
SHA-256:	617E32CA57507098771FD30AF6B9DCAB063448F6D7E0BC6D6557DD1895F80543

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\datarequestpackage_h-_7C7UzwdefXJT9njDBTQ2[1].js	
SHA-512:	CB107C09F9A32D85BF2AF714EE9BF7CE2649AA33E63C2255D4BBD281E3CDA8FBDFA2E58212E8004AEEAAB4DD8C94543F82187C7673189CACBDD5CD8C26C53F7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/datarequestpackage_h-_7C7UzwdefXJT9njDBTQ2.js
Preview:	!function(){function e(e){function t(e){return e&&e.state==l&&(e.prev&&(e.prev.next=e.next),e.next&&(e.next.prev=e.prev),D==e&&(D=e.next),$==e&&($=e.prev),e.state=u,e.prev=e.next=null,y--),e}function a(e){if(e&&e.state==u){var r=$;r?(r.next=e,e.prev=r):D=e,$=e,e.state=l,y++}}function f(){!q&&!b&&y&&x>w&&(b=window.setTimeout(g,s))}function v(e){var r=(new Date).getTime()-e<i;return r}function g(){var e=(new Date).getTime();for(b=0,q=!0;y>0&&x>w;){var r=D;if(r&&x>w?(o.assert(r.state===l,"Task was not in a pending state and we were just about to execute it."),r=m(t(r))):r=null,r&&!v(e)){break.}}q=!1,f()}function m(e){if(e){o.assert(void 0!=e.id&&!A[e.id],"Task didn't have an id or was already active!"),w++,A[e.id]=e,e.startTime=(new Date).getTime(),e.state=c;var r=e.exec(function(r){T(e,r)});r||T(e)}return e}function T(e,r){e.state===c&&(w--,o.assert(A[e.id],"A task is being completed without being in the active task list."),delete A[e.id],r&&"number"==typeof r?(e.state=d,e.timeoutId=wind

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\favicon_a_eupayfgghqiai7k9sol6lg2[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
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico
Preview:	.............h(..f...HH..........(..00......h....6.. ....=..............@..........(....A..(....................(..................................."P...""""""""""""""""""""""""""""""""" ...33333333333333333333333333333333""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333""""""""""""""""""""""""""""""""" ...33333333333333333333333333333""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"" ...3333333333333333333333333333333""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333""""""""""""""""""""""""""""""""" ...33333333333333333333333333333""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\jquery-1.11.2.min[1].js</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>ASCII text, with very long lines</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>95931</td></tr>
<tr><td>Entropy (8bit):</td><td>5.394232486761965</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:5P1vk7i6GUHdXXeyQazBu+4HhiO2AEeLNFoqqhJ7SerN5sVI6xcBgPv7E+nzms9d:A4Ud4qhJvNPqcB47MfWWca98HrB</td></tr>
<tr><td>MD5:</td><td>5790EAD7AD3BA27397AEDFA3D263B867</td></tr>
<tr><td>SHA1:</td><td>8130544C215FE5D1EC081D83461BF4A711E74882</td></tr>
<tr><td>SHA-256:</td><td>2ECD295D295BEC062CEDEBE177E54B9D6B19FC0A841DC5C178C654C9CCFF09C0</td></tr>
<tr><td>SHA-512:</td><td>781ACEDC99DE4CE8D53D9B43A158C645EAB1B23DFDFD6B57B3C442B11ACC4A344E0D5B0067D4B78BB173ABBDED75FB91C410F2B5A58F71D438AA6266D048[illegible]98A</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js</td></tr>
<tr><td>Preview:</td><td>/*! jQuery v1.11.2 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k={},l="1.11.2",m=function(a,b){return new m.fn.init(a,b)},n=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,o=/^-ms-/,p=/-([\da-z])/gi,q=function(a,b){return b.toUpperCase()};m.fn=m.prototype={jquery:l,constructor:m,selector:"",length:0,toArray:function(){return d.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var b=m.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a,b){return m.each(this,a,b)},map:function(a){return this.pushStack(m.map(this,function(b,c){ret</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2[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):	80144
Entropy (8bit):	5.421376219099593
Encrypted:	false
SSDEEP:	1536:vZ2N4/PzS0zdqm4NVmVtfB6aTJDIO5XxV7FyTDQIp8a+fNNnbt:Ay+0LmmBt7c1+Rfbt
MD5:	5F50584B68D931B8BB85F523F15BAA14

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2[1].js	
SHA1:	FAF4BD348F40016BCE0ABF54F167C7923B303ABB
SHA-256:	3C829DCF48768082A6177B77AE4E499337ED4C8BD056705CDB1E979F7B6EFCE5
SHA-512:	EB01573B9152D93400C7BCDC0C3746B58E8F5F8BA7A4C033D3A30D688E307543979402CAD4A19249391BA3113466F562D20A521BBEFFB7864AEBEB18FDB79BC1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2.js?v=1
Preview:	/*!---------- START OF THIRD PARTY NOTICE ----------....This file is based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise. .... * Knockout JavaScript library v3.3.0.. * (c) Steven Sanderson - http://knockoutjs.com/.. * License: MIT (http://www.opensource.org/licenses/mit-license.php)....Provided for Informational Purposes Only....MIT License ....Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the Software)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\latest[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Segoe UI Semibold family
Category:	downloaded
Size (bytes):	30643
Entropy (8bit):	7.976822258863597
Encrypted:	false
SSDEEP:	768:UOtV1asJ9G0dAdnVrKX/HkVJRPvkgxYZ4Zoe:bLasJ9G0u0fk/RnkgxGof
MD5:	E812BA8B7E2A657F2B70CFACE93C7682
SHA1:	2F02CDDBB483F9B11BBBE74C3CA917A4C345FBAD
SHA-256:	3330C1DEAC468874238DD0C6BF902179A8731EDA8A208C7D01DAC0AB1EAE1BC9
SHA-512:	354B2DB12BC1D67F26F94352B0B663DAD64C46C107454FC19CFEA01C54BB09340BC26C06DE1B96FF826F5287CE246A6317722BAE41B72B63BA86FDAF844BA94E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://i.s-microsoft.com/fonts/segoe-ui/west-european/semibold/latest.eot?
Preview:	.w...v.....X.....LP#...B..... .....".S.e.g.o.e. .U.I. .S.e.m.i.b.o.l.d.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .5...3.2...".S.e.g.o.e. .U.I. .S.e.m.i.b.o.l.d.....H .P..lb.7^.....U.D.-..iu...:4P\..GLFM.Y.#?.;..-...~}_).z{.rmD.1".$.....{.t.....=...!cK...%.~.....g.....j.9S....6. ..n..V.]pz...e.....#X...=,.p.F..6&.VR...k$~J..n....7.....K.8..T.....x..J.....#.J .XaQ.Q%_{3..xr.... 0Dm...k..Ep.....>..?Pk!KB..C...Q.q..1=6<,.S.F.&B..J.....ya2b."S.....6.2.....H.....*..09A...Tb/.&.d..#.E.:.E.(..I5.M..444d.1.....K..I...I.O..VBb....:..b..Mh.'=4.d/..o.k.mMm.....bx..!..S.@E.....>@:..k.JCas..7."..uG3hR.h..w..8W>.4.....pX....J..a....}.Y.....(>H^=.`=.mg*.!....w'....J.<.ob..3A .../.....5%.'....XS0a.....I.Ia....a...=..g..... {V1+..")7$2 O..!bb.=..|.s.1..2qm..#.O.....+E(I..1....EgQ.....E)R.m.?.8.q...J.G.@!f..n.F.r#..(..2p.?.9.8..?.d]..s..0.9.f..A...r.iq....x.g.aO....S.....R0i..BT.yl.".<k...:&Ja.\.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\latest[2].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Segoe UI Light family
Category:	downloaded
Size (bytes):	28315
Entropy (8bit):	7.9724193003797
Encrypted:	false
SSDEEP:	384:+R0Z7+bHAtrQ1yBFbgqLct7rJhhPLLkHsrvSzaJu4mI3n5o+MmKCxDg6iT7jdVye:+uNUAtE3phPLLFTiMu+pxCjHyGEQ9zL
MD5:	17DFE73CB9C64527F7248B0A24DB317D
SHA1:	345198B9239FCDAF038FB2D3A919E4724037DBAA
SHA-256:	AD75FB92B2EBCE6C37640F03E1AB96A752F388BCE60C877ADE4780B13839E8C4
SHA-512:	421B56D93E9BD5E4B4449DD0FCDEE8D531087FD484C91530AAF0A67EDEA33D5AC2F14A7F4966C528C0F130F17F26629FCAB9F8AB47E950CEB5B9F1A827EA0728
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.eot?
Preview:	.n...m.....LP#...B..... .....S.e.g.o.e. .U.I. .L.i.g.h.t.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .5...3.2.....S.e.g.o.e. .U.I. .L.i.g.h.t.....K..e..66.....U.D.-..iu...4P\..GLFM..C?.;..-...~|...P..\.(..)RI.....>.>..CE..SsV.jPR...H.....].R..&.n.hT.....x.....q .....wA[....F.....c.".....Zed..>.?...`..3...B..W....R....F.j....v..'?.5.k^.....+..a...)..._].x.#QSi.....|<t....k.;..Hv1.G...L$.9....5.t.:...V.Y.....|.@....B.....P`..2.Z.0....2`.FR.MF8.x....GP0..$:....PYm.22..."S."1.*j[=.=.mR.*.....j....&.4...k..].1@..y$....."y..C..g7..k.B*. ..V..F\...G.m.jK ...O....b.Qlo...!.N.V....t.[..p.N..~@1d...YX.."....R_i.4.$j.P..U....u9...<..6..4%.....9`.....S...N.Y..L..B$2\.E.vhe...n..h..5..Z..K?.H..S...2..=R..x.....EX.2.....$."....It8..z.+.h ..$.2*T....}Z../....p..b0ae.qq.(-v1..E.!.l".a..p.).;..8t..7..^..W...4A.D\eOb$.....b.NI.Pe.#$.O38....,....g..&|...B{...].....9..u.8..~Y...3.X..ff.,.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\latest[3].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Segoe UI family
Category:	downloaded
Size (bytes):	35047
Entropy (8bit):	7.975792390307888
Encrypted:	false
SSDEEP:	768:I6ibzTDpOGuAJ63YB9eSzDtQEspfAzyNyuBmOfAJYCM:/iPMYJ4GEAZoTyglcM
MD5:	CAD76E4816AF6890C9BFD02A6D1EA899

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\latest[3].eot	
SHA1:	9EDC91541C31034FCE0D83AABBAAD4C314CD3D33
SHA-256:	D5794223D1A062E5DBE6C34C1994C8CE3792B24AFD5218D0644CB1F53DA4BE58
SHA-512:	24983A5856C2B4D8CBE2A4BD233A93B266A03D4218942E1D1733B33B65AB7A504AF0AC31DE2F1E69F6FF8CCD7A169CD4555539D34FFF8DE4CB8C98DB2DB2C 63
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot?
Preview:	...=.....LP#...B..... .....S.e.g.o.e. .U.I.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .5...3.2.....S.e.g.o.e. .U.I.....RV.z..;~.....U.D.-..iu...N4P\..GLFM .Y.?.;..-...~~....Ox.M..".$.._.....g..sC*2..4W.....9AGc.[a..*.rCl,..@..U_..L...e..Ru.J.-.f..3.....S`.A.....K<;...n.Y...rli.....([...W...5k.....^K.G...U.@....2H..B.)N0w.....C..9..... ....#.l2,4..6y.3$b....K.wx...I.$E..?3.8.c...,x..t.wa.O....4.c...!..+.<EM...2T.>\..]4.A.H.;..G.....W.:.?...Z".....e....8....84.L,.)0..y.Xdd.Pa.@.&.o(.I.q.yF...[.y.m(D...(....T.....,A.;q.... .w.$..C..a.. .Y.O?{..0...'1.;C.,.....W..Q-..'.5tD@9..U...E4e.&_...S.Y...\)b.s.rIR.....%..R..KU O..{.0(.....^Q\^!.et...Kf%..K...}.1...S.{.....3p..]...|Y...w..|JeS$..k.....>(8 .ZlV..N.). c...Z.K.\..q.....'S.j.....9...._..E.#s*#.....[.....DJ^.L7../1...+U.qG.....-..MM..q....L..c...^...e....<h..:..`.jz..fb.Ha.....k.....e\)g..\."..M

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\lightweightsignuppackage_mStdClDku7grp_TX7Xaf-g2[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):	186220
Entropy (8bit):	5.388358175132689
Encrypted:	false
SSDEEP:	3072:6KrpW4hD//gaVS2Xu5Ly4yToqlla99ws3bIvXSgq4CF90EtT:ZWfdy4yToqlla99ws3sBET
MD5:	992B5D0A50E4BBB82BA7F4D7ED769FFA
SHA1:	6E473485198E0BA116E6761B8B97BD5E751F4FDB
SHA-256:	A1143F7455003238C2803B63B1322F84E4D9607ED246B10DE256FE764E3F2542
SHA-512:	7E475EA30A2B27C04650F35A536BB8ABE5A2C1517BA2F5FB068D7BB8B80C5F8F4DE8B39EE656E8CB2F28555475AF7D772271A84CDC6D2472C0AB26197AA1CE CC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/lightweightsignuppackage_mStdClDku7grp_TX7Xaf-g2.js?v=1
Preview:	function Encrypt(e,t,n,a){var i=[];switch(n.toLowerCase()){case"chgsqsa":if(null==e||null==t){return null}i=PackageSAData(e,t);break;case"chgpwd":if(null==e||null==a){ret urn null}i=PackageNewAndOldPwd(e,a);break;case"pwd":if(null==e){return null}i=PackagePwdOnly(e);break;case"pin":if(null==e){return null}i=PackagePinOnly(e);brea k;case"proof":if(null==e&&null==t){return null}i=PackageLoginIntData(null!=e?e:t);break;case"saproof":if(null==t){return null}i=PackageSADataForProof(t);break;c ase"newpwd":if(null==a){return null.}i=PackageNewPwdOnly(a)}if(null==i||"undefined"==typeof i){return i}if("undefined"!=typeof Key&&void 0!==parseRSAKeyFromString) {var r=parseRSAKeyFromString(Key)}var o=RSAEncrypt(i,r,randomNum);return o}function PackageSAData(e,t){var n=[],a=0;n[a++]=1,n[a++]=1,n[a++]=0;var i,r=t.leng th;for(n[a++]=2*r,i=0;r>i;i++){n[a++]=255&t.charCodeAt(i),n[a++]=(65280&t.charCodeAt(i))>>8}var o=e.length;for(n[a++]=o,i=0;o>i;i++){n[a++]=127&e.charCodeAt(i)}return n}function PackagePwdOn

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://signup.live.com/Resources/images/microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38 .119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392, 1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47. 081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0, 0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.61 1,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.9 52,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\override[1].css	
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):	1531
Entropy (8bit):	4.797455242405607
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\override[1].css	
SSDEEP:	24:Udf0F+MOu2UOqD3426TKgR2Yyk9696TkMYqdfskeEkeGk/ksuF9qaSm9qags:Ud8FYqTj36TKgR2Yyk9696TkMYO0keEW
MD5:	A570448F8E33150F5737B9A57B6D889A
SHA1:	860949A95B7598B394AA255FE06F530C3DA24E4E
SHA-256:	0BD288D5397A69EAD391875B422BF2CBDCC4F795D64AA2F780AFF45768D78248
SHA-512:	217F971A8012DE8FE170B4A20821A52FA198447FA582B82CF221F4D73E902C7E3AA1022CB0B209B6679C2EAE0F10469A149F510A6C2132C987F46214B1E2BBBC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://statics-marketingsites-eus-ms-com.akamaized.net/statics/override.css?c=7
Preview:	a.c-call-to-action:hover, button.c-call-to-action:hover{box-shadow:none!important}a.c-call-to-action:hover span, button.c-call-to-action:hover span{left:0!important}...c-call-to-action:not(.glyph-play):after { right: 0!important;} a.c-call-to-action:focus,button.c-call-to-action:focus{box-shadow:none!important}a.c-call-to-action:focus span,button.c-call-to-action:focus span{left:0!important;box-shadow:none!important}...theme-dark .c-me .msame_Header_name {color: #f2f2f2;}...pmg-page-wrapper .uhf div, .pmg-page-wrapper .uhf button, .pmg-page-wrapper .uhf a, .pmg-page-wrapper .uhf span, .pmg-page-wrapper .uhf p, .pmg-page-wrapper .uhf input {font-family: Segoe UI, SegoeUI,Helvetica Neue,Helvetica,Arial,sans-serif !important;}..@media (min-width: 540px) {.pmg-page-wrapper .uhf .c-uhfh-alert span, .pmg-page-wrapper .uhf #uhf-g-nav span, .pmg-page-wrapper .uhf .c-uhfh-actions span, .pmg-page-wrapper .uhf li, .pmg-page-wrapper .uhf button, .pmg-page-wrapper .uhf a, .pmg-page-wrapper .uhf #meC

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\privacystatement[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	328900
Entropy (8bit):	4.849916708233173
Encrypted:	false
SSDEEP:	3072:67698b1xiaNyN2d69v36WHkAd5C6ZNRrufSyIxqzEZC/Bd7ZENOxCQyZCqTeHwxD:6nxiM6TYs3Nu8iN1yZCSeHaagp
MD5:	D38AA0851775CE2358B5B988DA6C3E02
SHA1:	8CE60348228521D9EFA1D6D03FF237925AF6F8EA
SHA-256:	BA7D54436E3B8E3F0BC540E32015DC92F23CBD91A3D1782D415BE11B51A30815
SHA-512:	5CB2196211A05CF12A8044AB6EF4F0B55B2457FC2C416E2F9AFA0169156FC1F2C789FFBC256E9FDED8CED3B135D4D019CE705BD5B90644635911E1E034DD19E4
Malicious:	false
Reputation:	low
Preview:	.<!DOCTYPE html ><html xmlns:mscom="http://schemas.microsoft.com/CMSvNext" xmlns:md="http://schemas.microsoft.com/mscom-data" lang="en-us" xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta charset="utf-8" /><meta name="viewport" content="width=device-width, initial-scale=1.0" /><link rel="shortcut icon" href="https://www.microsoft.com/favicon.ico?v2" /><script type="text/javascript" src="https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js">...../// Third party scripts and code linked to or referenced from this website are licensed to you by the parties that own such code, not by Microsoft. See ASP.NET Ajax CDN Terms of Use - http://www.asp.net/ajaxlibrary/CDN.ashx... </script><script type="text/javascript" language="javascript">/*<![CDATA[*/if($(document).bind("mobileinit",function(){$.mobile.autoInitializePage=!1}),navigator.userAgent.match(/IEMobile\/10\.0/)){var msViewportStyle=document.createElement("style");msViewpo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\script[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):	121249
Entropy (8bit):	5.258860505507024
Encrypted:	false
SSDEEP:	1536:+JXd+YOlaYOyguxH6GdXJKjZtQ3EBJ0PYmwYmEZeQ8Wt2Db7ACu8J8lvC7CQBgAc:ed+YOlaYOyguxHbdX2nX5PaCfey
MD5:	B110D87662D257F657ABCCEF7AF5CD09
SHA1:	FD7519D842B6344448E6F1D69DFFA5F896FAE4A6
SHA-256:	65E82E7414D88BC864191400084C24DA27052E7A61F9F3C1F1EFDFEE433D558C
SHA-512:	EF429EE8701D0748DE81CEE25D15C9674487691ACA8982F6D43DA519E1CDFD5082D9DE5A71D1FB457250828433856BAB4A2CE7E035152FE9C16224FA433D35D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=0502864a-b6ef-2f14-9f8e-267004d3a4e0_c5ea3348-55af-729a-2641-14f0312bacf3_742bd11f-3d7c-9955-3df5-f02b66689699_cb9d43d2-fbae-5b5c-827f-72166d6b87fc_49488e0d-6ae2-5101-c995-f4d56443b1d8_7dea7b90-4334-c043-b252-9f132d19ee19_38aa9ffb-ddb5-75be-6536-a58628f435f5_e3e65a0a-c133-43e7-571d-2293e03f85e6_4ca0e9dc-a4de-17ba-f0de-d1d346cb99e2_06310cd8-41c6-3b11-4645-b4884789ed70_5c27e8aa-9347-969e-39ac-37a4de428a8d_d6872b5a-5310-a73c-7cb3-227a3213a1c5_be92d794-4118-193f-9871-58b72092a5ac_64c742e2-b29c-b6c1-fdd9-accf33ec40bd_cf2ceca9-3467-a5b3-d095-68958eee6d4c_cec39dd8-f1d3-56f1-abfc-a7db34ff7b46_ec5fa2c9-3950-ff57-a5c3-1fa77e0db190_d19f9592-65df-bcc9-e30e-439b875c3381_76a3d06f-f11f-77ef-9bfd-6227ba750200_5e1caa45-461c-3b04-f88b-8cd50af16db5_c2dceda8-20b4-7d3f-13b6-9cac67d7df17_914fa41b-cc86-d3b0-4e15-2fdfa357bcc7_40c6c884-da6e-7c2c-081f-4a7dfe7c7245_ae79ba96-1a9d-debd-a5b1-f3067213b9b8
Preview:	function getQueryValue(n,t){var r=new RegExp("[\\?&]"+t+"=([^&#]*)","gi"),i=r.exec(n);return i==null?"":decodeURIComponent(i[1].replace(/\+/g," "))}function getStore(n){var t="ClosestStore.asmx",r,i;$(".store-geo[data-GeoStoreLocalServiceURL]").length&&(t=$(".store-geo").first().attr("data-GeoStoreLocalServiceURL"));i="POST";typeof n!="undefined"&&(r={latitude:JSON.stringify(n.coords.latitude),longitude:JSON.stringify(n.coords.longitude)},t=t+"ClientGeo",i="GET");$.ajax({url:t,type:i,timeout:5e3,data:r,contentType:"application/json; charset=UTF-8",dataType:"json",error:function(){$(".store-geo").remove();$(".store-editorial").fadeIn(1e3)},success:function(n){if(typeof n!="undefined"&&typeof n.d!="undefined"&&typeof n.d.City!="undefined"&&n.d.City!=""&&n.d.StoreUrl!="undefined"&&n.d.StoreUrl!=""){var t=$(".store-geo:first").text();$(".store-geo a").html(t+" "+n.d.City);$(".store-geo a").attr("href",n.d.StoreUrl);$(".store-editorial").remove();$(".store-geo").fadeIn(1e3)}else $(".store-g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\signup[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\signup[1].htm	
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	206867
Entropy (8bit):	4.961309128026567
Encrypted:	false
SSDEEP:	1536:O8X71E5eFzlF70UgGZiKV5um/ZFpoBM1SSBY25AQhxGDLgFbDJqlgdmy:ruRWiAum/ZFpoBWBd1xGPgFbSgQy
MD5:	839629AD033C65999188F72D9D76F2CC
SHA1:	C721D666228AC3D162A18B34F79559B2AACFAA8A
SHA-256:	6FE66D2AE47B86A887E1310EBAD3C97F8B08A5E74596D617DC9FCD65329DA958
SHA-512:	B59B589C8BA71D29AE9704E6E0E02119665FF1F374CD7BC38C863DF50509938BC774787C31704FA1AD5E649A29C7397C3B7A6A11A248B311171DF8E9A8EC9E6
Malicious:	false
Reputation:	low
Preview:	.. Copyright (C) Microsoft Corporation. All rights reserved. -->....<!DOCTYPE html>..<html lang="en" xml:lang="en" class="m_ul" dir="ltr" style="">.. <head>.. <link rel="preconnect" href="https://acctcdn.msauth.net" crossorigin>..<link rel="preconnect" href="https://acctcdn.msauth.net" crossorigin>..<meta http-equiv="x-dns-prefetch-control" content="on">..<link rel="dns-prefetch" href="//acctcdn.msauth.net">..<link rel="dns-prefetch" href="//acctcdn.msftauth.net">..<link rel="dns-prefetch" href="//acctcdnmsftuswe2.azureedge.net">..<link rel="dns-prefetch" href="//acctcdnvzeuno.azureedge.net">.... <title>Microsoft account</title>.. <meta http-equiv="Content-Type" content="text/html;charset=utf-8"/><meta name="referrer" content="origin"/><meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=2.0, minimum-scale=1.0, user-scalable=yes"/><meta name="format-detection" content="telephone=no"/>.. <link rel="shortcut icon" href="https://acctcdn.msau

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\2_vD0yppaJX3jBnfbHF1hqXQ2[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1864
Entropy (8bit):	5.222032823730197
Encrypted:	false
SSDEEP:	48:yvswNIBLBpJawmMH44log6gw/MHm7pJroog6gwkMH9Xog6gwdMHdqdyqog7C:ykfXYx+odPcs9B
MD5:	BC3D32A696895F78C19DF6C717586A5D
SHA1:	9191CB156A30A3ED79C44C0A16C95159E8FF689D
SHA-256:	0E88B6FCBB8591EDFD28184FA70A04B6DD3AF8A14367C628EDD7CABA32E58C68
SHA-512:	8D4F38907F3423A86D90575772B292680F7970527D2090FC005F9B096CC81D3F279D59AD76EAFCA30C3D4BBAF2276BBAA753E2A46A149424CF6F1C319DED5A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/images/2_vD0yppaJX3jBnfbHF1hqXQ2.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6z" fill="url(#A)"/><path d="M394.2 1815.6c746.58 0 1351.8-493.2 1351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 1815.6 394.2 1815.6z" fill="url(#B)"/><path d="M1548.6 1885.2c631.92 0 1144.2-417.45 1144.2-932.4S2180.52 20.4 1548.6 20.4 404.4 437.85 404.4 952.8s512.276 932.4 1144.2 932.4z" fill="url(#C)"/><path d="M265.8 1215.6c690.246 0 1249.8-455.595 1249.8-1017.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUnits="userSpaceOnUse" gradientTransform="translate(1466.4 393.6) rotate(90) scale(1401.6 1720.8)"><stop stop-color="#107c10"/><stop offset="1" stop-color="#c4c4c4" stop-opacity="0"/></radialGradient><r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\app[1].css	
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):	262641
Entropy (8bit):	4.9463902181496096
Encrypted:	false
SSDEEP:	3072:u+Vd0pBbqPLYoyjFkxD2hAYwJb8lLm731Ss:u+Vd0DePLYoyjFkxD2hAYwJbZLM31Ss
MD5:	7C593B06759DB6D01614729D206738D6
SHA1:	0D4F76D10944933B8DDECFFE9691081439A77A3C
SHA-256:	F7D9FB0479DE843CF3FB0B78FC56BBB9E30BF0A238C6F79D9209FA8B22EFB574
SHA-512:	EF91B610CF17A17AAFB48984B4403EF175EB86096E3F12E23AE8D4C7C96EF60ED14DA3F69721E095CD2ACE3F0A06190186D000992823814BB906F7FB3576C2C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.onestore.ms/cdnfiles/external/oneui/oneui1.16.2/dist/css/app.css
Preview:	@font-face {. font-family: "wf_segoe-ui_normal";. src: url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot");. src: url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot?#iefix") format("embedded-opentype"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.woff") format("woff"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.ttf") format("truetype"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.svg#web") format("svg");. font-weight: normal;. font-style: normal; }..@font-face {. font-family: "wf_segoe-ui_light";. src: url("//i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.eot");. src: url("//i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.eot?#iefix") format("embedded-opentype"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.woff") format("woff"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.ttf") format("truetype

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\converged.v2.login.min_rayhgcterrtxpnvapp3erg2[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\converged.v2.login.min_rayhgcterrtxpnvapp3erg2[1].css	
Category:	downloaded
Size (bytes):	107668
Entropy (8bit):	5.291456416114907
Encrypted:	false
SSDEEP:	1536:QpHDglkuhw+ExiazA/PWrF7qvEAFiQcpmWGQvz6yVUn1:lEJ4yVU1
MD5:	440CA18024DE46B4D73E7540A4FDDE46
SHA1:	C4FF7AF4E1558E081DF52C1E61A5D63D0BE577C7
SHA-256:	EA6449D448A48495C557755AF39701567925CEAFC30E06FBA05F65E723C91AA3
SHA-512:	3A3A9D58E0E9645E2399CD83F53D842CBA47AA42EBAFECAB9AE29784AA7CE8A842F0CE89DFE8E35E3CD7387ADCFB66DA68BFCD2EDCAE9560C5E9F775A770 3B37
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/converged.v2.login.min_rayhgcterrtxpnvapp3erg2.css
Preview:	/*! Copyright (C) Microsoft Corporation. All rights reserved. *//*!.-- START OF THIRD PARTY NOTICE ---..This file based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise...//--.twbs-bootstrap-sass (3.3.0).//---..The MIT License (MIT)..Copyright (c) 2013 Tw Inc..Permission is hereby granted, free of charge, to any person

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/images/favicon.ico?v=2
Preview:	.............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(....................(....................................."P.."""""""""""""""""""""" ...3 3333333333333333333333333333333"""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""" ...3333333333333333333333333333333"""" """""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""" ...33333333333 33333333333333333333"""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""" """""""" ...3333333333333333333333333333333"""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""" ...3333333333333333333333 333333333"""""""""""""""""""""" ...3333333333333333333333333333333""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\favicon[2].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
Reputation:	low
IE Cache URL:	http://https://signup.live.com/Resources/images/favicon.ico
Preview:	.............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(....................(....................................."P.."""""""""""""""""""""" ...3 3333333333333333333333333333333"""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""" ...3333333333333333333333333333333"""" """""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""" ...33333333333 33333333333333333333"""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""" """""""" ...3333333333333333333333333333333"""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""" ...3333333333333333333333 333333333"""""""""""""""""""""" ...3333333333333333333333333333333""""""""""""""""""""

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\mwfmdl2-v3.54[1].woff	
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
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/mwf/_h/v3.54/mwf.app/fonts/mwfmdl2-v3.54.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$.....x...x.c`.Pf.....:....Q.B3_dHc..`e.bdb... .`@..`...../9.\|... V...)00...-.Wx...S....._..m.m.m.m.m;e..y.~.....<p..a.0t.&...a.pa.0B.1..F...Q.ha.0F.3.....q.xa.0A.0L.&...I.da.0E.2L....i.ta.0C.1..f...Y.la.0G.3.....y.\|a..@X0,.....E.ba.DX2,....e .ra..BX1..V...U.ja..FX3.....u.za..A.0l.6...M.fa.E.2l....m.va..C.1..v...].na..G.3.....}.~a.p@80.....C.a..pD82.....c.q..pB81..N...S.i..pF83.....s.y..pA.0\.....K.e..pE.2\....k.u..pC.1..n...[. m..pG.3.....{.}...@x0<.....G.c...Dx2<....g.s...Bx1..^...W.k...Fx3.....w.{...A.0\|.>...O.g...E.2\|....o.w...C.1..~..._.o..08.....?..0$.....x...mL.U.....9.x.`[...&BF@X...V.h.Z..h. .....`n....[..U

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\override[1].css	
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):	1531
Entropy (8bit):	4.797455242405607
Encrypted:	false
SSDEEP:	24:Udf0F+MOu2UOqD3426TKgR2Yyk9696TkMYqdfskeEkeGk/ksuF9qaSm9qags:Ud8FYqTj36TKgR2Yyk9696TkMYO0keEW
MD5:	A570448F8E33150F5737B9A57B6D889A
SHA1:	860949A95B7598B394AA255FE06F530C3DA24E4E
SHA-256:	0BD288D5397A69EAD391875B422BF2CBDCC4F795D64AA2F780AFF45768D78248
SHA-512:	217F971A8012DE8FE170B4A20821A52FA198447FA582B82CF221F4D73E902C7E3AA1022CB0B209B6679C2EAE0F10469A149F510A6C2132C987F46214B1E2BBBC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://statics-marketingsites-wcus-ms-com.akamaized.net/statics/override.css?c=7
Preview:	a.c-call-to-action:hover, button.c-call-to-action:hover{box-shadow:none!important}a.c-call-to-action:hover span, button.c-call-to-action:hover span{left:0!important}...c-call-to-action:not(.glyph-play):after { right: 0!important;} a.c-call-to-action:focus,button.c-call-to-action:focus{box-shadow:none!important}a.c-call-to-action:focus span,button.c-call-to-action:focus span{left:0!important;box-shadow:none!important}...theme-dark .c-me .msame_Header_name {color: #f2f2f2;}...pmg-page-wrapper .uhf div, .pmg-page-wrapper .uhf button, .pmg-page-wrapper .uhf a, .pmg-page-wrapper .uhf span, .pmg-page-wrapper .uhf p, .pmg-page-wrapper .uhf input {font-family: Segoe UI, SegoeUI,Helvetica Neue,Helvetica,Arial,sans-serif !important;}..@media (min-width: 540px) {.pmg-page-wrapper .uhf .c-uhfh-alert span, .pmg-page-wrapper .uhf #uhf-g-nav span, .pmg-page-wrapper .uhf .c-uhfh-actions span, .pmg-page-wrapper .uhf li, .pmg-page-wrapper .uhf button, .pmg-page-wrapper .uhf a, .pmg-page-wrapper .uhf #meC

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\shell.min[1].css	
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):	82190
Entropy (8bit):	5.036904170769404
Encrypted:	false
SSDEEP:	1536:tJzwN0CbUTqI34/9w6/Qua+1IGEbjBko230WBYT:vyA
MD5:	1F9995AB937AC429A73364B4390FF6E8
SHA1:	81998DCC6407CEB5CEF236AD52B9F2A3A9528D3B
SHA-256:	49E5166F40D8586714F86E08AB76A977199DF979357147A0E81980A804151C2A
SHA-512:	6669AE352FF46DB734BB8F973D1C0527C3A5EC4119D534AAE4C33F29EFF970168ED5FE200A05D4E1B6A2EC0E090E2207549B926317D489DC7664B0D9C208546
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.onestore.ms/cdnfiles/onestorerolling-1510-19009/shell/v3/scss/shell.min.css
Preview:	@charset "UTF-8";@font-face{font-family:'wf_segoe-ui_normal';src:local("Segoe UI");src:url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot");src:url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot?#iefix") format("embedded-opentype"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.woff") format("woff"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.ttf") format("truetype"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.svg#web") format("svg");font-weight:normal;font-style:normal}@font-face{font-family:'wf_segoe-ui_semilight';src:url("//i.s-microsoft.com/fonts/segoe-ui/west-european/semilight/latest.eot");src:url("//i.s-microsoft.com/fonts/segoe-ui/west-european/semilight/latest.eot?#iefix") format("embedded-opentype"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/semilight/latest.woff") format("woff"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/semilight/latest.ttf")

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\style[1].css	
Category:	downloaded
Size (bytes):	836
Entropy (8bit):	4.940950417710206
Encrypted:	false
SSDEEP:	24:Cn5ZoK2kNMCJZ4ZVaeao1DphsILHJNM2WXgEXgf0Xgm:u5dxJZ4+BWIIPLQ73/
MD5:	2AC383F4677A1036C8EA4289F99A31E3
SHA1:	E65967B9273029CDDD5A5F8DF9E61DACF89CF11C
SHA-256:	2206A95E6BAC7C185CC54638EBF0B0089CBC27FF729B45AC63C968CFE4991AA4
SHA-512:	9E61D4E2B42A1BC776C5649ECD2E32A1CE1ACEDA929E8C013D20BE95D12B7B56864FD588D6117E6410988331F85E21815E2E135030F49BEA2A244F872570DBE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSStyles/style.csx?k=4627136a-bd68-db6e-30c9-37cf96c98eee
Preview:	body .grid,.body-open .grid,.grid h3,.grid .h3,.grid .header-small,.grid strong,.grid .body-tight-2,.grid h1,.grid .h1,.grid .header-large,.grid .caption{font-family:"Segoe UI"}.grid{max-width:1600px !important}.c-uhfh-actions,.c-uhfh-gcontainer-st .all-ms-nav,.glyph-global-nav-button{display:none !important}.shell-header-wrapper,.shell-footer-wrapper,.shell-category-nav,.shell-notification .shell-notification-grid-row{max-width:1180px !important}.PsTitle{font-family:Segoe UI,sans-serif;margin-right:.3em !important;font-size:2em;display:inline-block;vertical-align:top;margin-left:-.02em}.childModule{margin-left:8% !important}.CollectingYourInfoRightNav{display:none}html[dir=rtl] .m-r-md{margin-right:0;margin-left:10px}html[dir=rtl] .m-l-md{margin-left:0;margin-right:10px}html[dir=rtl] .m-r-bl{margin-right:0;margin-left:40px}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\ux.converged.login.strings-en.min_xw0hy9kamszck8doonyj8g2[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):	40083
Entropy (8bit):	5.407937223904449
Encrypted:	false
SSDEEP:	768:g2MPDo7yAF1tlfretkdTKNa8DRN2ym+d/PngTehlOb8GYTPRUbx3Tg/ayyG3ljkR:EgF1tlfretkdTKNa8DRN2ym+d/PngTeK
MD5:	5F0D07CBD90032C65C2BC0E8A27609F2
SHA1:	082E891C48B28D510ECD672A7573D01474B2B5B6
SHA-256:	34BD1E67DD38AF6F495BC90D22733FF5A8308161FFE2548FAF93C1D39DDDF5D6
SHA-512:	D0609CF9F3DA4C8249A23CEC35C0A445AB3B6B9BBB9088D5254512060A782E731369CE413C6359DDF48FE3D1CD5BFBDCBBD2E62B239664EE07C784CC0F6B42A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/ux.converged.login.strings-en.min_xw0hy9kamszck8doonyj8g2.js
Preview:	!function(e){function o(n){if(i[n])return i[n].exports;var t=i[n]={exports:{},id:n,loaded:!1};return e[n].call(t.exports,t,t.exports,o),t.loaded=!0,t.exports}var i={};return o.m=e,o.c=i,o.p="",o(0)}([function(e,o,i){i(2);var n=i(1),t=i(5),r=i(7),a=r.StringsVariantId,_=r.AllowedIdentitiesType;n.registerSource("str",function(e,o){if(e.WF_STR_SignupLink_AriaLabel_Text="Create a Microsoft account",e.WF_STR_SignupLink_AriaLabel_Generic_Text="Create a new account",e.CT_STR_CookieBanner_Link_AriaLabel="Learn more about Microsoft's Cookie Policy",e.WF_STR_HeaderDefault_Title=o.iLoginStringsVariantId===a.CombinedSigninSignupV2WelcomeTitle?"Welcome":"Sign in",e.STR_Footer_IcpLicense_Text=".ICP.13015306.-10",o.oAppCobranding&&o.oAppCobranding.friendlyAppName){var i=o.fBreakBrandingSigninString?"to continue to {0}":"Continue to {0}";e.WF_STR_App_Title=t.format(i,o.oAppCobranding.friendlyAppName)}switch(o.oAppCobranding&&o.oAppCobranding.signinDescription&&(e.WF_STR_Default_Desc=o.oAppCobrand

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:	F0A10A4C1CA4BAC8A2DBD41F80BBE1F83D767A4D289B149E1A7B6E7F4DBA41236C5FF244350B04E2EF485FDF6EB774B9565A858331389CA3CB474172465EB3BF
Malicious:	false
Reputation:	low
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(var 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\OR0WKIO1\2_vD0yppaJX3jBnfbHF1hqXQ2[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\2_vD0yppaJX3jBnfbHF1hqXQ2[1].svg	
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1864
Entropy (8bit):	5.222032823730197
Encrypted:	false
SSDEEP:	48:yvswNIBLBpJawmMH44log6gw/MHm7pJroog6gwkMH9Xog6gwdMHdqdyqog7C:ykfXYx+odPcs9B
MD5:	BC3D32A696895F78C19DF6C717586A5D
SHA1:	9191CB156A30A3ED79C44C0A16C95159E8FF689D
SHA-256:	0E88B6FCBB8591EDFD28184FA70A04B6DD3AF8A14367C628EDD7CABA32E58C68
SHA-512:	8D4F38907F3423A86D90575772B292680F7970527D2090FC005F9B096CC81D3F279D59AD76EAFCA30C3D4BBAF2276BBAA753E2A46A149424CF6F1C319DED5A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://signup.live.com/Resources/images/2_vD0yppaJX3jBnfbHF1hqXQ2.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6z" fill="url(#A)"/><path d="M394.2 1815.6c746.58 0 1351.8-493.2 1351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 1815.6 394.2 1815.6z" fill="url(#B)"/><path d="M1548.6 1885.2c631.92 0 1144.2-417.45 1144.2-932.4S2180.52 20.4 1548.6 20.4 404.4 437.85 404.4 952.8s512.276 932.4 1144.2 932.4z" fill="url(#C)"/><path d="M265.8 1215.6c690.246 0 1249.8-455.595 1249.8-1017.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUnits="userSpaceOnUse" gradientTransform="translate(1466.4 393.6) rotate(90) scale(1401.6 1720.8)"><stop stop-color="#107c10"/><stop offset="1" stop-color="#c4c4c4" stop-opacity="0"/></radialGradient><r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\50-f1e180[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	133618
Entropy (8bit):	5.224613249025047
Encrypted:	false
SSDEEP:	3072:1f/HuFVppxvIeJ0i9d1EwgXA9JKi5DCE5n:1f/Hu/FIeRxn
MD5:	04053017246241626B6706F1AB465531F
SHA1:	1C034383716BCE493E28BFFF0DD2C27F049CC558
SHA-256:	A5DD3C05EFED81BBF60B618C070A7746F030147590EE0EDD74459AC4E53955FD
SHA-512:	9D81E61D3B0AED73F7A64D0344E432AEAAAB057655CFEB040348FA876693E618A434D63727F1E4AA1118276740C7102FD412637B46752665B78EB3C81A53915A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-eus-prod/shell/_scrf/js/themes=default/54-af9f9f/c0-247156/de-099401/e1-a50eee/e7-954872/d8-97d509/f0-251fe2/46-be1318/77-04a268/11-240c7b/63-077520/a4-34de62/bb-d7480b/db-bc0148/dc-7e9864/6d-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/79-499886/7e-cda2d3/b2-7087f0/e5-08f1c0/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/50-f1e180?ver=2.0&iife=1
Preview:	(function(){/**. * @license almond 0.3.3 Copyright jQuery Foundation and other contributors.. * Released under MIT license, http://github.com/requirejs/almond/LICENSE. */ .var requirejs,require,define,__extends;(function(n){function r(n,t){return w.call(n,t)}function s(n,t){var o,s,f,e,h,p,c,b,r,l,w,k,u=t&&t.split("/"),a=i.map,y=a&&a["*"]||{};if(n){ for(n=n.split("/"),h=n.length-1,i.nodeIdCompat&&v.test(n[h])&&(n[h]=n[h].replace(v,"")),n[0].charAt(0)===".."&&u&&(k=u.slice(0,u.length-1),n=k.concat(n)),r=0;r<n.length;r++)if(w=n[r],w===".")n.splice(r,1),r-=1;else if(w===".."){if(r===0||r===1&&n[2]===".."||n[r-1]==="..")continue;else r>0&&(n.splice(r-1,2),r-=2);n=n.join("/")}if((u||y)&&a){ for(o=n.split("/"),r=o.length;r>0;r-=1){if(s=o.slice(0,r).join("/"),u)for(l=u.length;l>0;l-=1)if(f=a[u.slice(0,l).join("/")],f&&(f=f[s],f)){e=f;p=r;break}if(e)break;!c&&y&&y[s]&&(c=y[s],b=r)}!e&&c&&(e=c,p=b);e&&(o.splice(0,p,e),n=o.join("/"))}return n}function y(t,i){return function(){var r=b.call(arguments,0

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 CRLF line terminators
Category:	downloaded
Size (bytes):	2347
Entropy (8bit):	5.290031538794594
Encrypted:	false
SSDEEP:	48:gCgF0+kNL5iQ6+GhB+SYWzGuesAFcsGJOzgO6FIEv+sj+M++sx+suse+swsosmC0:gC3Na5+GX+Ti2XsYE2sqAsosushswsoB
MD5:	E86EF8B6111E5FB1D1665BCDC90888C9
SHA1:	994BF7651CB967CD9053056AF2D69ACB74DB7F29
SHA-256:	3410242720DE50B090D07A23AEE2DAD879B31D36F2615732962EC4CFA8A9D458
SHA-512:	2486B491681EE91A9CD1ECC9AA011A3FB34B48358C5D7A4D503A5357BC5CE4CA22999F918D40AC60A3063940D5F326FC7E4E5713D89D5C102DE68824E371B3AB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://login.live.com/Me.htm?v=3
Preview:	<script type="text/javascript">!function(n,t){for(var e in t)n[e]=t[e]}(this,function(n){function t(i){if(e[i])return e[i].exports;var s=e[i]={exports:{},id:i,loaded:!1};return n[i].call(s.exports,s,s.exports,t),s.loaded=!0,s.exports}var e={};return t.m=n,t.c=e,t.p="",t(0)}([function(n,t){function e(n){for(var t=g[c],e=0,i=t.length;e<i;++e)if(t[e]===n)return!0;return!1}function i(n){if(!n)return null;for(var t=n+"=",e=document.cookie.split(";"),i=0,s=e.length;i<s;i++){var o=e[i].replace(/^\s*(\w+)\s*=\s*/,"$1=").replace(/(\s+$)/,"");if(0===o.indexOf(t))return o.substring(t.length)}return null}function s(n,t,e){if(n)for(var i=n.split(":"),s=null,o=0,a=i.length;o<a;++o){var l=null,c=i[o].split("$");if(0===o&&(s=parseInt(c.shift()),!s))return;var p=c.length;if(p>=1){var f=r(s,c[0]);if(!f||e[f])continue;l={signInName:f,idp:"msa",isSignedIn:!0}}if(p>=3&&(l.firstName=r(s,c[1]),l.lastName=r(s,c[2])),p>=4){var g=c[3],m=g.split("|");l.otherHashedAliases=m}if(p>=5){var h=parseInt(c[4],16);h&&(l.

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:	D4F6E49C854E15FE48D6A1F1A03FDA93218AB8FCDB2C443668E7DF478830831ACC2B41DAEFC25ED38FCC8D96C4401377374FED35C36A5017A11E63C8DAE5C87
Malicious:	false
Reputation:	low
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:xmpmeta 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:A00BC638840A11E68CBEB97C2156C7FD" xmp:CreatorTool="Adobe Photoshop CC 2015.5 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:A2C931A470A111E6AEDFA14578553B7B" 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...I.....wg.y.[k/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\cf-7c36ab[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):	168646
Entropy (8bit):	5.044051581582224
Encrypted:	false
SSDEEP:	3072:OzCPZkTP3bDLH0tfRqQ0xtLfj4ZDSIpTt813viY8R1j35Ap7LQZLPPJH7PAbOCxR:clZAXLkeedh
MD5:	0DCFF2779D4542C11AD9C9C19DF8328D
SHA1:	D7EFAE8E66FA6B4C335826BFD8C56C6F142E4254
SHA-256:	440D8292ABDF80DD6E8A9D9FAEA83367CE57BD1A1A8D153EDC358DB5F97EFF35
SHA-512:	CC747AA36ADEE4CBA4236F01820CE9661214C649DCF23227D7CF9187E24F2D15DBA43E9B706B30DC3D55060E08601575EAB0256306AEA28F3544BAD4BC33E93
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-wcus-prod/west-european/shell/_scrf/css/themes=default.device=uplevel_web_pc/93-de417f/39-6894a8/60-0f9daa/9c-879d19/5f-d422a2/ea-c61049/a7-5072ba/cf-7c36ab?ver=2.0
Preview:	@charset "UTF-8";./*! | 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 */.body{margin:0}.context-uh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\dropdown_caret_KXSZjGsyILZaoTf0sI9X-A2[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	224
Entropy (8bit):	5.066130335315081
Encrypted:	false
SSDEEP:	6:tI9mc4slz2lWjVRqtmd9QA0ZcTKhqnR40Y:t44lWjVRqtnA0Zcq6R40Y
MD5:	2974998C6B3220B65AA137F4B08F57F8
SHA1:	F4F08DA689179DE68EE40CD12ECDCC5AC54B3979
SHA-256:	96D52BD03E244A44931A541A807067792D638DD29EC14A87A78F2BE85D12D19A
SHA-512:	6B4F2439CA99109A7C97828E5972A8E7C7FCA3745B2FB4738EBD9329A99234A8CD3BC4C0C48B5BAA917D4BAA64CDAEB5D74456DEFDDDA3E07FAA803283BE0287
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/images/dropdown_caret_KXSZjGsyILZaoTf0sI9X-A2.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="36" height="36" viewBox="0 0 36 36"><title>assets</title><path d="M18,22.484l-8-8,.969-.968L18,20.547l7.031-7.031.969.968-8,8Z"/><rect width="36" height="36" fill="none"/></svg>

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
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/favicon.ico
Preview:	.............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(....................(....................................."P...""""""""""""""""""""""""""""""" ...3 3333333333333333333333333333""""""""""""""""""""""""""""""" ...3333333333333333333333333333""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""" """"""""""""""""""""""""""""" ...3333333333333333333333333333""""""""""""""""""""""""""""""" ...3333333333333333333333333333""""""""""""""""""""""""""""""" ...33333333333 33333333333333333""""""""""""""""""""""""""""""" ...3333333333333333333333333333""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""" """"""""" ...3333333333333333333333333333""""""""""""""""""""""""""""""" ...3333333333333333333333333333""""""""""""""""""""""""""""""" ...33333333333333333333 333333333""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\favicon[2].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
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/favicon.ico?v2
Preview:	.............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(....................(....................................."P...""""""""""""""""""""""""""""""" ...3 3333333333333333333333333333""""""""""""""""""""""""""""""" ...3333333333333333333333333333""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""" """"""""""""""""""""""""""""" ...3333333333333333333333333333""""""""""""""""""""""""""""""" ...3333333333333333333333333333""""""""""""""""""""""""""""""" ...33333333333 33333333333333333""""""""""""""""""""""""""""""" ...3333333333333333333333333333""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""" """"""""" ...3333333333333333333333333333""""""""""""""""""""""""""""""" ...3333333333333333333333333333""""""""""""""""""""""""""""""" ...33333333333333333333 333333333""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\icons[1].eot</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>Embedded OpenType (EOT), icons family</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>4388</td></tr>
<tr><td>Entropy (8bit):</td><td>5.568378803379191</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>96:2WZx42qACoApC6do8MPOGiN4mER38GTDfO/fv:1x42qAHAo6VMPi6mcTy</td></tr>
<tr><td>MD5:</td><td>77E1987DF3A0274C5A51E3C55CEE7C98</td></tr>
<tr><td>SHA1:</td><td>9B0FE96AF141AB09183F386F65BC627B8C396460</td></tr>
<tr><td>SHA-256:</td><td>EF04649D4D068673CF0FA47EF4C45C8BE291E703F4EC5FC0E507F17839120AA2</td></tr>
<tr><td>SHA-512:</td><td>B1E0CFB515FF2298799BA54574899D27B1FC043F66CC4E9591C504F88273B98697B99ED25955DB84986B39ED9F51864611833DC88064B14C29ADC020FBF6E295</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://assets.onestore.ms/cdnfiles/external/oneui/oneui1.16.2/dist/fonts/icons/icons.eot?</td></tr>
<tr><td>Preview:</td><td>$................................LP..........................G....................i.c.o.n.s.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .1...0.....i.c.o.n.s................ OS/2@.Mn...(...Vcmap.1.........Jglyf..........dhead. 9.........6hhea.$.........$hmtx@...........loca". h...L...Bmaxp.3.`....... name............post{NK.. ....G..._.<............|.......|.......................... .T............ ....D.l...H.D.l...................................PfEd.@...D...........(. ....</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd[1].svg	
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/shared/1.0/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38 .119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392, 1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47. 081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0, 0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.61 1,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.9 52,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\oneds_Xr2D7Nex80v7A-8bxF8jgQ2[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):	82052
Entropy (8bit):	5.312628857785992
Encrypted:	false
SSDEEP:	768:paVnZVNvlcxbEFWEI3+d8lLCNMnSpjaQ2Z8q2G/b8bSqY4gs8Lh1mAXbQON9fAvC:cuediuNMk1T/qTlAvrQUAluA
MD5:	5EBD83ECD7B1F34BFB03EF1BC45F2381
SHA1:	CD1E0062A04B11EEB36586766BF5144955250E65
SHA-256:	4C57821AA26F21DEEBC39E3C750BC4FE246C430E5E50F4ADD0CFF53943C8C608
SHA-512:	9B56B2F1F301AD65D03514E1EC557830501805CBB81A891A518601898AE4F3C8A4C063D64036C2E8F1E539E5989CB608D535A01552BCADF008B53D1B699E9E88
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/oneds_Xr2D7Nex80v7A-8bxF8jgQ2.js?v=1
Preview:	/*!.. * 1DS JS SDK Core, 2.3.4.. * Copyright (c) Microsoft and contributors. All rights reserved... * (Microsoft Internal Only).. */..!function(e,n){"object"==typeof expo rts&&"undefined"!=typeof module?n(exports):"function"==typeof define&&define.amd?define(["exports"],n):n(e.oneDS=e.oneDS||{})}(this,function(c){"use strict";var i="functi on",o="object",n="undefined",a="prototype",s="hasOwnProperty";function e(){return typeof globalThis!==n&&globalThis?globalThis:typeof self!==n&&self?self:typeof window!==n&&window?window:typeof global!==n&&global?global:null}function r(e){var n=Object.create;if(n)return n(e);if(null==e)return{};var t=typeof e;if(t!==o&&t!==i)thr ow new TypeError("Object prototype may only be an Object:"+e);function r(){}return r[a]=e,new r}function t(e){for(var n,t=1,r=arguments.length;t<r;t++)for(var i in n=argu ments[t])Object[a][s].call(n,i)&&(e[i]=n[i]);return e}var u=function(e,n){return(u=Object.setPrototypeOf||{__proto__:[]}instanceof Array&&function(e,n){e.__prot

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\servicesagreement[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	209820
Entropy (8bit):	5.165015326786186
Encrypted:	false
SSDEEP:	6144:G+TZaZEzF0a6OGYL0seowg6ehsymCJ2i/T9VTSfaTHgJi7eshMcgGJ3AQ:GKZaZEzX6OGYQseowg6ehsymCJ2i/pV7
MD5:	F313A181CD449B9794333352C0EE20AB
SHA1:	869B133A92C3E1FE511CBFA5D06C00AF91C5CB78
SHA-256:	C81A004DBE79E9FA73981A88FF253EAA2E0B153A493B3B2C9077DD7FDB06BC79
SHA-512:	71841D04B0CD85F0D1B16CC08F13FA6A1228B1D54FD9C8963B58C92B6563AF6733403425B0EB380DCBB646B6B49D4E93A697F3E064F069D88A64C14650F22E83
Malicious:	false
Reputation:	low
Preview:	.<!DOCTYPE html ><html xmlns:mscom="http://schemas.microsoft.com/CMSvNext" xmlns:md="http://schemas.microsoft.com/mscom-data" lang="en-us" xmlns="http ://www.w3.org/1999/xhtml"><head><meta name="viewport" content="initial-scale=1.0, width=device-width" /><meta http-equiv="X-UA-Compatible" content="IE=edge" /><title>Microsoft Services Agreement</title><meta name="Title" content="Microsoft Services Agreement" /><meta name="CorrelationVector" content="cJgmsKF8 N0OglqBV.1" /><meta name="Description" content="" /><meta name="MscomContentLocale" content="en-us" /><link href="https://www.microsoft.com/onerfstatics/marketingsites-wcus-prod/west-european/shell/_scrf/css/themes=default.device=uplevel_web_pc/93-de417f/39-6894a8/60-0f9daa/9c-879d19/5f-d422a2/ea-c61049/a7-5072ba/cf-7c36ab?ver=2.0" rel="stylesheet" type="text/css" media="screen" /><link href="https://statics-marketingsites-wcus-ms-com.akamaized.net/statics/override.css?c=7" rel="stylesheet" type="text/css" media="screen" /><link rel

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\style[1].css	
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	137436
Entropy (8bit):	5.360850019087837
Encrypted:	false
SSDEEP:	1536:+Fk5W00zHVaAgrBmeZCstBwB/BxBf9e969j9S9h919g9Z9C9f9g9Z9e979Q9t9Vp:+Fk5W003MC/
MD5:	D0519383C16A2B2D2879BFBF15845F0C
SHA1:	B2FBBC365B2CA853B1CBEAAA0F10BB05148ED9AA
SHA-256:	046BA9FDD7992751785036A03AB6EDD3052465C23C2BAD1ADC80905DC6AA39A9
SHA-512:	2DB8E6E4AD75F756D0B70071EC49EA4FF54360AFDAAC007C0FFD5ACF575961E661DD275329347210AD71206885A50DA2E58F12CE84E6C7A3BC3D5EDD81E3B5 BE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSStyles/style.csx?k=3c9ade18-bc6a-b6bd-84c3-fc69aaaa7520_899796fc-1ab6-ed87-096b-4f10b915033c_e8d8727e-02f3-1a80-54c3-f87750a8c4de_6e5b2ac7-688a-4a18-9695-a31e8139fa0f_b3dad3e4-0853-1041-fa46-2e9d6598a584_fc29d27f-7342-9cf3-c2b5-a04f30605f03_28863b11-6a1b-a28c-4aab-c36e3deb3375_907fa087-b443-3de8-613e-b445338dad1f_a66bb9d1-7095-dfc6-5a12-849441da475c_1b0ca1a3-6da9-0dbf-9932-198c9f68caeb_ef11258b-15d1-8dab-81d5-8d18bc3234bc_11339d5d-cf04-22ad-4987-06a506090313_50edf96d-7437-c38c-ad33-ebe81b170501_8031d0e3-4981-8dbc-2504-bbd5121027b7_3f0c3b77-e132-00a5-3afc-9a2f141e9eae_aebeacd9-6349-54aa-9608-cb67eadc2d17_0cdb912f-7479-061d-e4f3-bea46f10a753_343d1ae8-c6c4-87d3-af9d-4720b6ea8f34_a905814f-2c84-2cd4-839e-5634cc0cc383_190a3885-bf35-9fab-6806-86ce81df76f6_05c744db-5e3d-bcfb-75b0-441b9afb179b_8beffb66-d700-2891-2c8d-02e40c7ac557_b1fe3f15-7512-0a8f-a55b-b316245621b5_f9c8eff0-3e34-2c33-6c0d-1fa7c5077eec
Preview:	@font-face{font-family:'wf_segoe-ui_light';src:url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/light/latest.eot');src:local("Segoe UI Light"),local("Segoe WP Light"),url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/light/latest.eot?#iefix') format('embedded-opentype'),url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/light/latest.woff') format('woff'),url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/light/latest.ttf') format('truetype'),url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/light/latest.svg#web') format('svg');font-weight:normal;font-style:normal}@font-face{font-family:'wf_segoe-ui_normal';src:url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/normal/latest.eot');src:local("Segoe UI"),local("Segoe"),local("Segoe WP"),url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/normal/latest.eot?#iefix') format('embedded-opentype'),url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/normal/latest.w

C:\Users\user\AppData\Local\Temp\~DF71AF7237989E274B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47210604896768327
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lof9lof9lW9y+VhVFMMd:kBqoIAe9y+VhVnd
MD5:	93B84DBA1BE1B581E505F18C0057B9BE
SHA1:	7EAD23C934FCDDB968735D9F22F3AC64093AD7A4
SHA-256:	297B210605BE2D8FB66DCC4DA093703F7CEEF8ED3772A7E267B300F1D9881E0F
SHA-512:	7E8BAF44F742433C9DDF1C74C479872E18E48D66B627CEB62612D2AE87A3BD7A2EB8150CF9917A593C9B24F2CC037779E00073A9089415DE695735793E43218C
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFB66D0A2BAC6D7BF1.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	98230
Entropy (8bit):	2.682242518215066
Encrypted:	false
SSDEEP:	1536:ugu01pBLOgu08pBL0pBLXpBL9pBLbpBL9pBLApBLTpBLapBLb:jpDWezhXhafMb
MD5:	0EC6D19D83BB47D205E9F5872CD5CB70
SHA1:	BEEB9096259AC376E7571D42DC81A7F40C3AA462
SHA-256:	352764C607E0BB421723471013719A91B5631CEE63B734151671087D08A76BD5
SHA-512:	85F0E3A3C213B5BB0988EE4F3E4ECED651A8AB155449302E93DD1480517C2E0DE5DC26E2FF74B0C9D8924E395CA7FC1699A8CA8B7C3A2ABB7DDEB4059C3F3 AB1
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFBBE7D503EFF5E58B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe

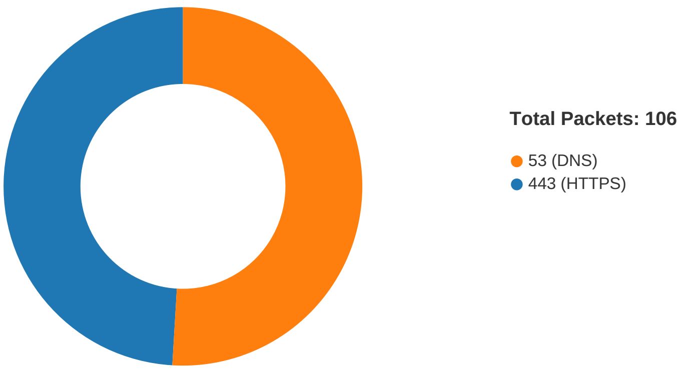
C:\Users\user\AppData\Local\Temp\~DFBBE7D503EFF5E58B.TMP	
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.3845852182362226
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA2mDQnRKJ:kBqoxxJhHWSVSEab2giU
MD5:	AB09ECD741D338488D74FC8BED94DE8E
SHA1:	746F395E3608053D069D613273FDCE2B4A19F969
SHA-256:	95248013C555D945BFF310608EBDD8AA27DB3F200EB4D5BBAA4461BC386D9B1B
SHA-512:	090D34D569B7F9A3AA194795319CCEE390350F66171D038D8FF1843D79406619BBE14BA46EE2372DA7D4EF19B7DD60F52E0A1D58B012E47F8EF4AC1E77C2DC5 B
Malicious:	false
Reputation:	low
Preview:	..............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 04:26:52.154542923 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.154762030 CET	49739	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.194402933 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.194592953 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.194628000 CET	443	49739	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.194789886 CET	49739	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.195633888 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.197041988 CET	49739	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.235399961 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.236498117 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.236538887 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.236578941 CET	443	49738	152.199.23.37	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 04:26:52.236608028 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.236624002 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.236696005 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.236735106 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.236742020 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.236844063 CET	443	49739	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.238394022 CET	443	49739	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.238436937 CET	443	49739	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.238472939 CET	443	49739	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.238498926 CET	443	49739	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.238523960 CET	443	49739	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.238523960 CET	49739	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.238604069 CET	49739	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.238615990 CET	49739	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.238622904 CET	49739	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.238630056 CET	49739	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.327964067 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.344521999 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.344868898 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.368096113 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.368141890 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.368269920 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.368308067 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.384444952 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.384598970 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.387768030 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.387810946 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.387850046 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.387886047 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.387902021 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.387932062 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.387933016 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.387938023 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.387943029 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.387974977 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.387999058 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.388012886 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.388031006 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.388050079 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.388072014 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.388087988 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.388101101 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.388123989 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.388140917 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.388159990 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.388175011 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.388196945 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.388211012 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.388243914 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.388252020 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.388289928 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.388297081 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.388328075 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.388351917 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.388365984 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.388401031 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.388403893 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.388418913 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.388441086 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.388457060 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.388478041 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.388494968 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.388514042 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.388530970 CET	49738	443	192.168.2.4	152.199.23.37

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 04:26:52.388561964 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.388571978 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.388603926 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.388618946 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.388641119 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.388658047 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.388676882 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.388693094 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.388715029 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.388727903 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.388739109 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.388767004 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.388776064 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.388786077 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.388832092 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.404676914 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.408159971 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.408210993 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.408252954 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.408260107 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.408267975 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.408303976 CET	443	49738	152.199.23.37	192.168.2.4
Jan 14, 2021 04:26:52.408322096 CET	49738	443	192.168.2.4	152.199.23.37
Jan 14, 2021 04:26:52.408360958 CET	49738	443	192.168.2.4	152.199.23.37

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 04:26:44.845726967 CET	55854	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:26:44.893831968 CET	53	55854	8.8.8.8	192.168.2.4
Jan 14, 2021 04:26:45.719619036 CET	64549	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:26:45.769774914 CET	53	64549	8.8.8.8	192.168.2.4
Jan 14, 2021 04:26:46.508564949 CET	63153	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:26:46.556606054 CET	53	63153	8.8.8.8	192.168.2.4
Jan 14, 2021 04:26:47.598531008 CET	52991	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:26:47.646629095 CET	53	52991	8.8.8.8	192.168.2.4
Jan 14, 2021 04:26:49.209305048 CET	53700	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:26:49.257411957 CET	53	53700	8.8.8.8	192.168.2.4
Jan 14, 2021 04:26:50.226748943 CET	51726	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:26:50.284444094 CET	53	51726	8.8.8.8	192.168.2.4
Jan 14, 2021 04:26:51.249015093 CET	56794	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:26:51.313361883 CET	53	56794	8.8.8.8	192.168.2.4
Jan 14, 2021 04:26:51.553847075 CET	56534	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:26:51.623245955 CET	53	56534	8.8.8.8	192.168.2.4
Jan 14, 2021 04:26:52.088880062 CET	56627	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:26:52.151040077 CET	53	56627	8.8.8.8	192.168.2.4
Jan 14, 2021 04:26:56.343090057 CET	56621	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:26:56.402406931 CET	53	56621	8.8.8.8	192.168.2.4
Jan 14, 2021 04:26:58.964468956 CET	63116	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:26:59.020884037 CET	53	63116	8.8.8.8	192.168.2.4
Jan 14, 2021 04:26:59.813837051 CET	64078	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:26:59.864567041 CET	53	64078	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:01.143024921 CET	64801	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:01.190970898 CET	53	64801	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:02.022594929 CET	61721	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:02.070563078 CET	53	61721	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:02.816046000 CET	51255	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:02.866694927 CET	53	51255	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:03.588293076 CET	61522	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:03.639090061 CET	53	61522	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:04.566463947 CET	52337	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:04.614419937 CET	53	52337	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:05.454380035 CET	55046	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:05.502505064 CET	53	55046	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 04:27:07.685889006 CET	49612	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:07.744884014 CET	53	49612	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:10.046776056 CET	49285	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:10.094764948 CET	53	49285	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:11.073674917 CET	50601	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:11.134254932 CET	53	50601	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:12.920557022 CET	60875	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:12.989438057 CET	53	60875	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:15.091510057 CET	56448	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:15.147938967 CET	53	56448	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:15.217561960 CET	59172	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:15.277996063 CET	53	59172	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:15.815740108 CET	62420	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:15.874516010 CET	53	62420	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:17.198185921 CET	60579	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:17.201875925 CET	50183	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:17.207611084 CET	61531	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:17.209712029 CET	49228	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:17.257519007 CET	53	60579	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:17.268493891 CET	53	49228	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:17.269598007 CET	53	61531	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:17.272641897 CET	53	50183	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:17.290103912 CET	59794	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:17.346194983 CET	53	59794	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:19.815743923 CET	55916	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:19.873577118 CET	53	55916	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:20.241810083 CET	52752	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:20.292673111 CET	53	52752	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:20.380716085 CET	60542	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:20.388777018 CET	60689	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:20.443413973 CET	53	60542	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:20.448039055 CET	53	60689	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:20.885184050 CET	64206	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:20.927551985 CET	50904	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:20.941545963 CET	53	64206	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:20.985666990 CET	53	50904	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:21.246768951 CET	52752	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:21.305855036 CET	53	52752	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:21.876035929 CET	64206	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:21.932759047 CET	53	64206	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:22.250835896 CET	52752	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:22.301835060 CET	53	52752	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:22.891495943 CET	64206	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:22.947987080 CET	53	64206	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:24.266776085 CET	52752	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:24.317805052 CET	53	52752	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:24.907299042 CET	64206	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:24.963845968 CET	53	64206	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:28.115228891 CET	57525	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:28.171756029 CET	53	57525	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:28.283390999 CET	52752	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:28.334201097 CET	53	52752	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:28.602097988 CET	53814	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:28.658485889 CET	53	53814	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:28.923149109 CET	64206	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:28.971196890 CET	53	64206	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:29.130856037 CET	53418	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:29.191929102 CET	53	53418	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:29.742786884 CET	62833	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:29.799117088 CET	53	62833	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:30.166496038 CET	59260	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:30.225948095 CET	53	59260	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:30.678936958 CET	49944	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:30.735441923 CET	53	49944	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 04:27:31.179958105 CET	63300	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:31.236440897 CET	53	63300	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:31.771877050 CET	61449	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:31.828275919 CET	53	61449	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:32.447351933 CET	51275	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:32.503963947 CET	53	51275	8.8.8.8	192.168.2.4
Jan 14, 2021 04:27:32.864485979 CET	63492	53	192.168.2.4	8.8.8.8
Jan 14, 2021 04:27:32.923765898 CET	53	63492	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2021 04:26:51.249015093 CET	192.168.2.4	8.8.8.8	0xee35	Standard query (0)	protection .office.com	A (IP address)	IN (0x0001)
Jan 14, 2021 04:26:51.553847075 CET	192.168.2.4	8.8.8.8	0x7eb7	Standard query (0)	login.micr osoftonline.com	A (IP address)	IN (0x0001)
Jan 14, 2021 04:26:52.088880062 CET	192.168.2.4	8.8.8.8	0x193d	Standard query (0)	aadcdn.msf tauth.net	A (IP address)	IN (0x0001)
Jan 14, 2021 04:27:07.685889006 CET	192.168.2.4	8.8.8.8	0x186b	Standard query (0)	aadcdn.msf tauth.net	A (IP address)	IN (0x0001)
Jan 14, 2021 04:27:11.073674917 CET	192.168.2.4	8.8.8.8	0x8345	Standard query (0)	signup.live.com	A (IP address)	IN (0x0001)
Jan 14, 2021 04:27:12.920557022 CET	192.168.2.4	8.8.8.8	0xe99c	Standard query (0)	acctcdn.ms auth.net	A (IP address)	IN (0x0001)
Jan 14, 2021 04:27:17.207611084 CET	192.168.2.4	8.8.8.8	0xe774	Standard query (0)	ajax.aspne tcdn.com	A (IP address)	IN (0x0001)
Jan 14, 2021 04:27:20.388777018 CET	192.168.2.4	8.8.8.8	0x3f5e	Standard query (0)	assets.one store.ms	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2021 04:26:51.313361883 CET	8.8.8.8	192.168.2.4	0xee35	No error (0)	protection .office.com	protection.office.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 04:26:51.623245955 CET	8.8.8.8	192.168.2.4	0x7eb7	No error (0)	login.micr osoftonline.com	a.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 04:26:51.623245955 CET	8.8.8.8	192.168.2.4	0x7eb7	No error (0)	a.privatel ink.msiden tity.com	prda.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 04:26:51.623245955 CET	8.8.8.8	192.168.2.4	0x7eb7	No error (0)	prda.aadg. msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 04:26:52.151040077 CET	8.8.8.8	192.168.2.4	0x193d	No error (0)	aadcdn.msf tauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 04:26:52.151040077 CET	8.8.8.8	192.168.2.4	0x193d	No error (0)	cs1100.wpc .omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Jan 14, 2021 04:26:56.402406931 CET	8.8.8.8	192.168.2.4	0x3d4c	No error (0)	prda.aadg. msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 04:27:07.744884014 CET	8.8.8.8	192.168.2.4	0x186b	No error (0)	aadcdn.msf tauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 04:27:07.744884014 CET	8.8.8.8	192.168.2.4	0x186b	No error (0)	cs1100.wpc .omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Jan 14, 2021 04:27:11.134254932 CET	8.8.8.8	192.168.2.4	0x8345	No error (0)	signup.live.com	account.msa.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 04:27:11.134254932 CET	8.8.8.8	192.168.2.4	0x8345	No error (0)	account.ms a.msidentity.com	account.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 04:27:12.989438057 CET	8.8.8.8	192.168.2.4	0xe99c	No error (0)	acctcdn.ms auth.net	acctcdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 04:27:12.989438057 CET	8.8.8.8	192.168.2.4	0xe99c	No error (0)	scdn1efff. wpc.9da5e. alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 04:27:12.989438057 CET	8.8.8.8	192.168.2.4	0xe99c	No error (0)	sni1gl.wpc .alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2021 04:27:17.268493891 CET	8.8.8.8	192.168.2.4	0x16e2	No error (0)	consentdeliveryfd.azurefd.net	star-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 04:27:17.269598007 CET	8.8.8.8	192.168.2.4	0xe774	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 04:27:20.448039055 CET	8.8.8.8	192.168.2.4	0x3f5e	No error (0)	assets.onestore.ms	assets.onestore.ms.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
Jan 14, 2021 04:26:52.236578941 CET	152.199.23.37	443	192.168.2.4	49738	CN=aadcdn.msftauth.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	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 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		
Jan 14, 2021 04:26:52.238472939 CET	152.199.23.37	443	192.168.2.4	49739	CN=aadcdn.msftauth.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	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 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		
Jan 14, 2021 04:27:07.830251932 CET	152.199.23.37	443	192.168.2.4	49750	CN=aadcdn.msftauth.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	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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		
Jan 14, 2021 04:27:13.142395020 CET	152.199.21.175	443	192.168.2.4	49757	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 SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jan 03 01:00:00 CET 2021 Fri Mar 08 13:00:00 CET 2013	Mon Jan 03 00:59:59 CET 2022 Wed Mar 08 13:00:00 CET 2023	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		
Jan 14, 2021 04:27:13.144961119 CET	152.199.21.175	443	192.168.2.4	49758	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 SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jan 03 01:00:00 CET 2021 Fri Mar 08 13:00:00 CET 2013	Mon Jan 03 00:59:59 CET 2022 Wed Mar 08 13:00:00 CET 2023	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		
Jan 14, 2021 04:27:13.322382927 CET	152.199.21.175	443	192.168.2.4	49759	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 SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jan 03 01:00:00 CET 2021 Fri Mar 08 13:00:00 CET 2013	Mon Jan 03 00:59:59 CET 2022 Wed Mar 08 13:00:00 CET 2023	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		
Jan 14, 2021 04:27:13.327892065 CET	152.199.21.175	443	192.168.2.4	49760	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 SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jan 03 01:00:00 CET 2021 Fri Mar 08 13:00:00 CET 2013	Mon Jan 03 00:59:59 CET 2022 Wed Mar 08 13:00:00 CET 2023	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		
Jan 14, 2021 04:27:13.337459087 CET	152.199.21.175	443	192.168.2.4	49761	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 SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jan 03 01:00:00 CET 2021 Fri Mar 08 13:00:00 CET 2013	Mon Jan 03 00:59:59 CET 2022 Wed Mar 08 13:00:00 CET 2023	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=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		
Jan 14, 2021 04:27:13.337752104 CET	152.199.21.175	443	192.168.2.4	49762	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 SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jan 03 01:00:00 CET 2021 Fri Mar 08 13:00:00 CET 2013	Mon Jan 03 00:59:59 CET 2022 Wed Mar 08 13:00:00 CET 2023	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		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6768 Parent PID: 800

General

Start time:	04:26:50
Start date:	14/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff702100000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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: 6816 Parent PID: 6768

General

Start time:	04:26:50
Start date:	14/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6768 CREDAT:17410 /prefetch:2
Imagebase:	0x910000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: TokenBrokerCookies.exe PID: 5484 Parent PID: 6768

General

Start time:	04:26:55
Start date:	14/01/2021

Path:	C:\Windows\System32\TokenBrokerCookies.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\TokenBrokerCookies.exe <no_string> https://login.microsoftonline.com/0 tbauth://login.windows.net/?context=https%3A%2F%2Flogin.microsoftonline.com&request_nonce=AwABAAAAAAABAOz_AwD0_5mUgr2fSv4NxRRKhlfqZP9fUQosM2-hJX8votGQsH2PQuCecfPy-WPQWQ7eiFMW6_yA4NTsqZVOGf6tlSk0LBwgAA&rid=e376dce7-fc39-4390-87c3-8fadf9f10a00 ESTSUSERLIST %7b%22users%22%3a%5b%5d%7d login.microsoftonline.com / 0 1838406162 30864677 1
Imagebase:	0x7ff681eb0000
File size:	35840 bytes
MD5 hash:	17F27A76AC8E9869C8F1BE286D88570A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis