ID: 1447354
Cookbook: browseurl.jbs
Time: 21:29:39
Date: 24/05/2024
Version: 40.0.0 Tourmaline

Table of Contents

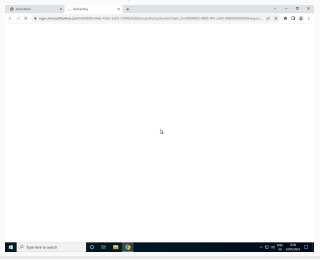
Windows Analysis Report

https://jmawireless-my.sharepoint.com

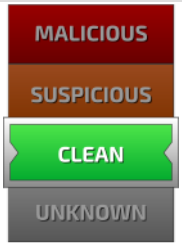
Overview

General Information

Sample URL:	http://https://jmawireless-my.sharepoint.com
Analysis ID:	1447354
Infos:	



Detection

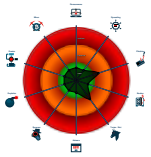


Score:	2
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected non-DNS traffic on DNS po…
- Detected suspicious crossdomain re…
- HTML body contains low number of …
- HTML title does not match URL

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 4600 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank" MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
  - chrome.exe (PID: 404 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2052 --field-trial-handle=2012,i,10823017092375802373,5579075643260688422,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8 MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
- chrome.exe (PID: 6424 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" "https://jmawireless-my.sharepoint.com" MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

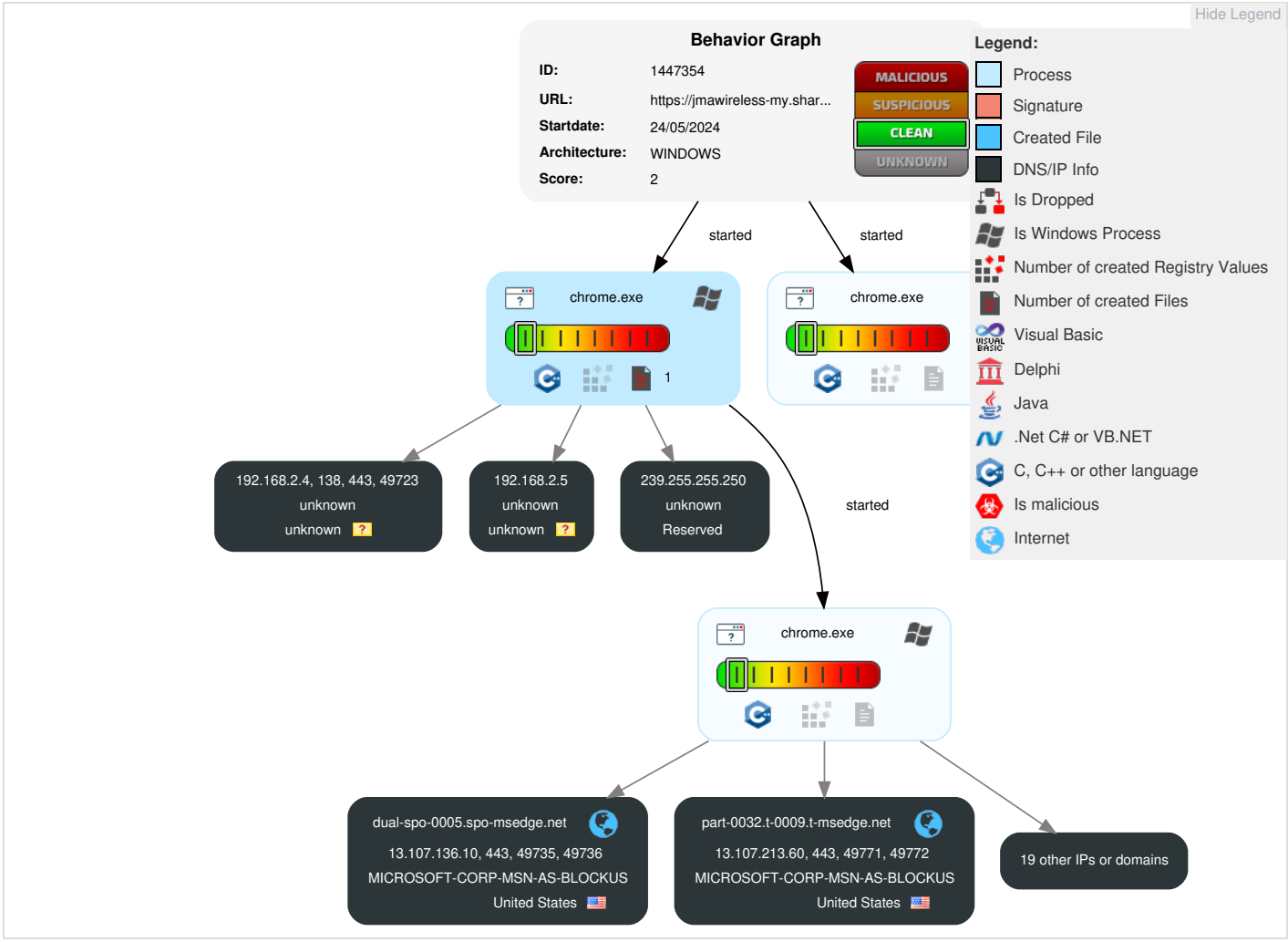
Joe Sandbox Signatures

There are no malicious signatures

Mitre Att&ck Matrix

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Process Injection	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	2 Non-Application Layer Protocol	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	3 Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	1 Ingress Tool Transfer	Traffic Duplication	Data Destruction

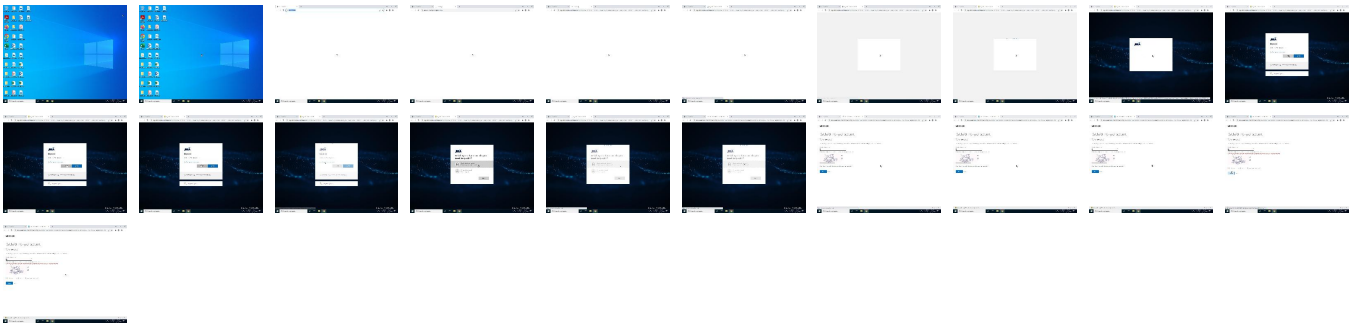
Behavior Graph

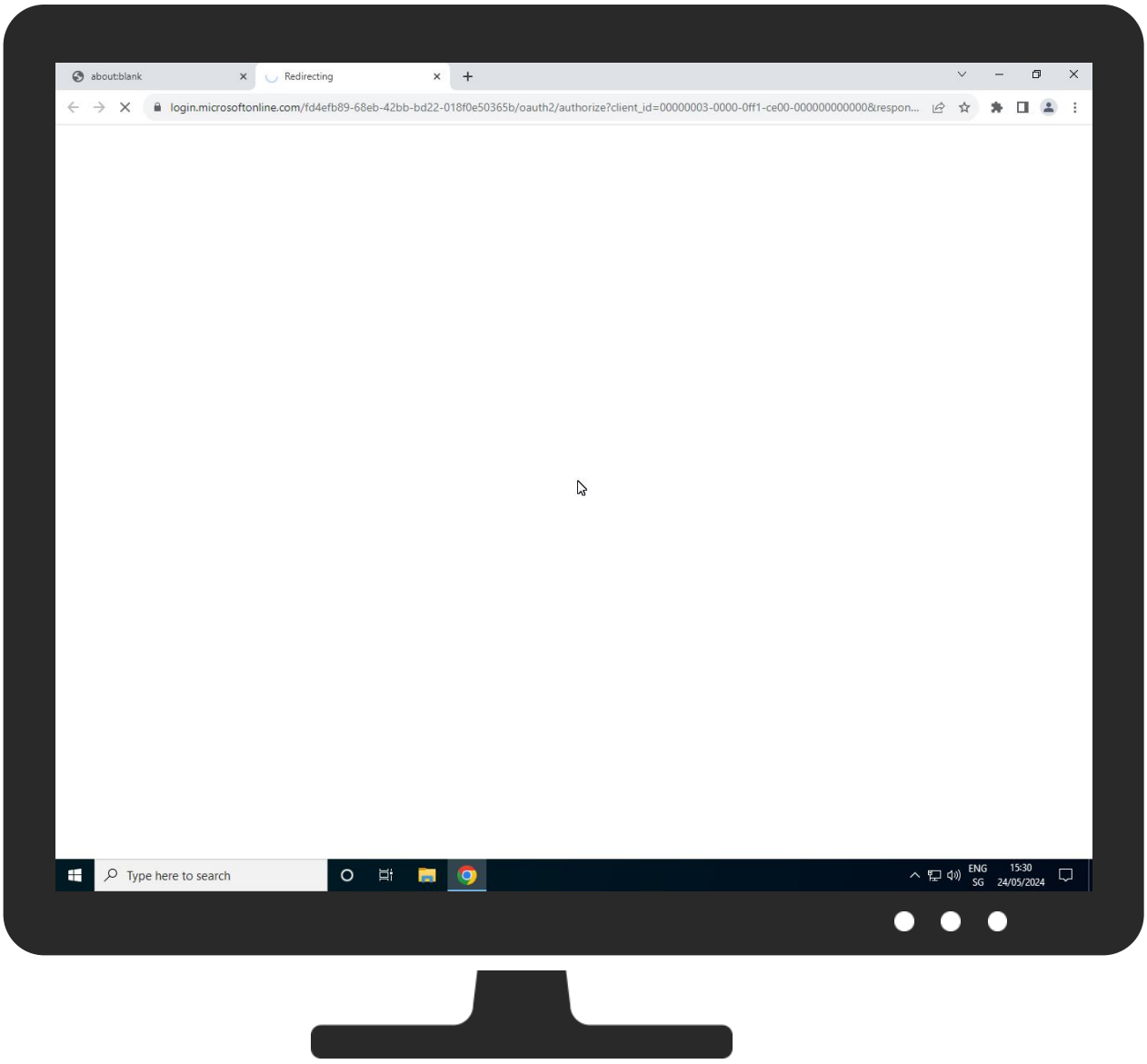


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://jmawireless-my.sharepoint.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://aadcdn.msftauth.net/shared/1.0/content/images/picker_account_msa_3b879963b4f70829fd7a25cbc9519792.svg	0%	URL Reputation	safe	
http://knockoutjs.com/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://login.windows-ppe.net	0%	URL Reputation	safe	
http://gsgd.co.uk/sandbox/jquery/easing/	0%	URL Reputation	safe	
http://https://login.microsoftonline.com	0%	URL Reputation	safe	
http://www.opensource.org/licenses/mit-license.php)	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/marching_ants_986f40b5a9dc7d39ef8396797f61b323.gif	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/marching_ants_white_8257b0707cbe1d0bd2661b80068676fe.gif	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/signin-options_3e3f6b73c3f310c31d2c4d131a8ab8c6.svg	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/picker_account_aad_a8332c62695d74843a11daf39a74e552.svg	0%	URL Reputation	safe	
http://feross.org	0%	URL Reputation	safe	
http://https://account.live.com/resetpassword.aspx	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/js/ConvergedLogin_PCore_T2EBBtMmyv072RjbQwNpoQ2.js	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/js/asyncchunk/convergedlogin_presetpasswordsplitter_f7fbb7540d7be2ae771b.js	0%	Avira URL Cloud	safe	
http://https://jmawireless-my.sharepoint.com/	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/converged.v2.login.min_9oft0ybq1qhuafkqh5wryq2.css	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/frameworksupport.min_oadrnc13magb009k4d20lg2.js	0%	Avira URL Cloud	safe	
http://https://github.com/douglascrockford/JSON-js	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/ux.converged.login.strings-en.min_vtf__v_j2jh3v2otg9k3lq2.js	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/js/asyncchunk/convergedlogin_pstringcustomizationhelper_ea3e62a2bdfb2b2ee8c8.js	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauthimages.net/dbd5a2dd-lfa6jvlreimgywhhs-c8kmaqnihskpfu3l8mv5xcc9i/logintenantbranding/0/illustration?ts=637441741242033826	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/watson.min_q5ptmu8aniymd4ftuqdkda2.js	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauthimages.net/dbd5a2dd-lfa6jvlreimgywhhs-c8kmaqnihskpfu3l8mv5xcc9i/logintenantbranding/0/bannerlogo?ts=637951424196423663	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/js/asyncchunk/convergedlogin_pcustomizationloader_8e14dcf0e3ff5580d170.js	0%	Avira URL Cloud	safe	
http://https://jmawireless-my.sharepoint.com/_layouts/15/Authenticate.aspx?Source=%2F	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/js/BssoInterrupt_Core_RY3pVDLvjU_KKLtTKxjDFA2.js	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/watsonsupportwithjquery.3.5.min_dc940oomzau4rsu8qesnvg2.js	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/js/asyncchunk/convergedlogin_pfetchsessionsprogress_7c1aa7609345f99e4914.js	0%	Avira URL Cloud	safe	
http://https://jmawireless-my.sharepoint.com/_forms/default.aspx?ReturnUrl=%2f_layouts%2f15%2fAuthenticate.aspx%3fSource%3d%252F&Source=cookie	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
part-0039.t-0009.t-msedge.net	13.107.246.67	true	false		unknown
dual-spo-0005.spo-msedge.net	13.107.136.10	true	false		unknown
cs1100.wpc.omegacdn.net	152.199.23.37	true	false		unknown
part-0032.t-0009.t-msedge.net	13.107.213.60	true	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.google.com	142.250.185.164	true	false		unknown
part-0039.t-0009.fb-t-msedge.net	13.107.226.67	true	false		unknown
fp2e7a.wpc.phicdn.net	192.229.221.95	true	false		unknown
autologon.microsoftazuread-sso.com	40.126.32.138	true	false		unknown
passwordreset.microsoftonline.com	unknown	unknown	false		unknown
identity.nel.measure.office.net	unknown	unknown	false		unknown
aadcdn.msftauth.net	unknown	unknown	false		unknown
login.microsoftonline.com	unknown	unknown	false		unknown
jmawireless-my.sharepoint.com	unknown	unknown	false		unknown
ajax.aspnetcdn.com	unknown	unknown	false		unknown
aadcdn.msftauthimages.net	unknown	unknown	false		unknown

Contacted URLs

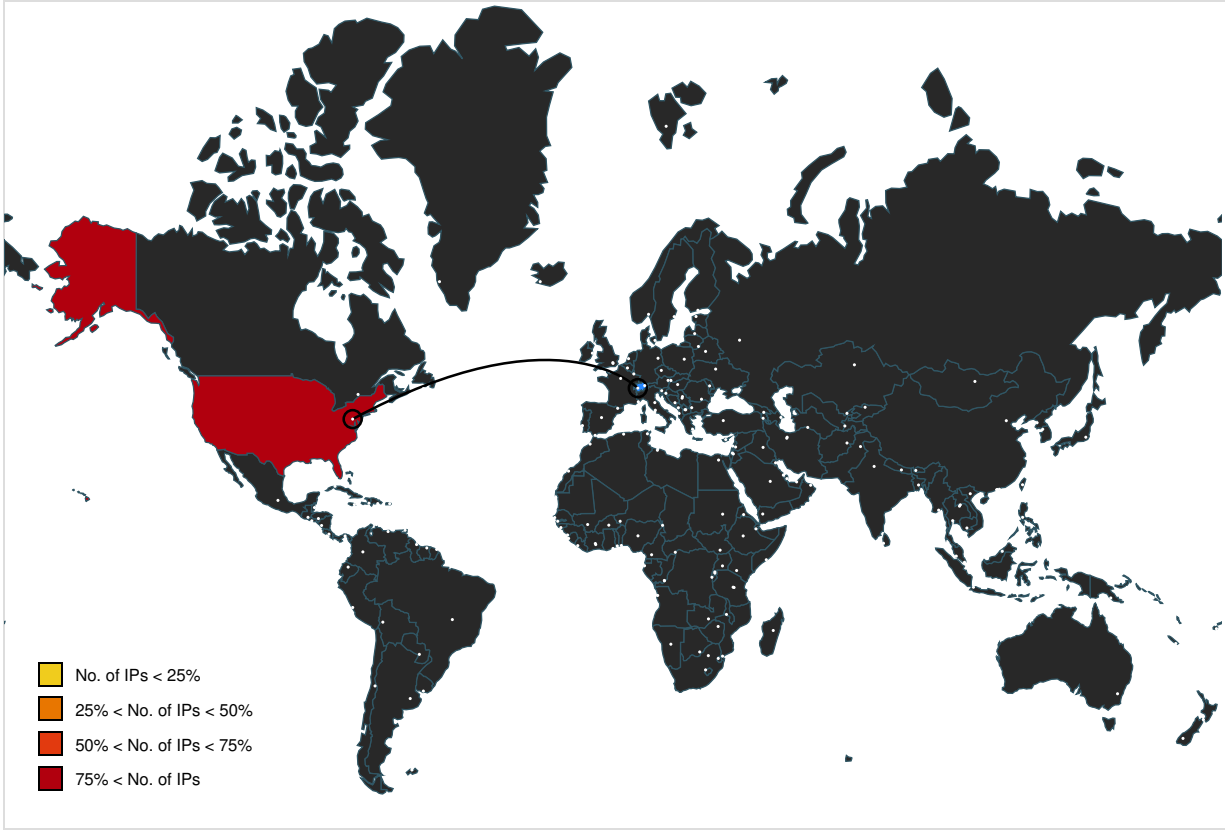
Name	Malicious	Antivirus Detection	Reputation
http://https://aadcdn.msftauthimages.net/dbd5a2dd-lfa6jvlreimgywhhs-c8kmaqnihskpfu3l8mv5xcc9i/logintenantbranding/0/illustration?ts=637441741242033826	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/js/asyncchunk/convergedlogin_presetpasswordsplitter_f7fbb7540d7be2ae771b.js	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/images/picker_account_msa_3b879963b4f70829fd7a25cbc9519792.svg	false	• URL Reputation: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/frameworksupport.min_oadrnc13magb009k4d20lg2.js	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/watson.min_q5ptmu8aniymd4ftuqdkda2.js	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/ux.converged.login.strings-en.min_vtf__v_j2jh3v2otg9k3lq2.js	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/js/asyncchunk/convergedlogin_pstringcustomizationhelper_ea3e62a2bdfb2b2ee8c8.js	false	• Avira URL Cloud: safe	unknown
http://https://passwordreset.microsoftonline.com/?ru=https%3a%2f%2flogin.microsoftonline.com%2ffd4efb89-68eb-42bb-bd22-018f0e50365b%2freprocess%3fctx%3drQQIARAAnVE_aNRgHE2aa-ydrT3q4ljOTj1z-ZJ8Sb4cdMi_04ras3-gnsiRP1_aeJdLmqTtXUsXdRAE6eyidnDoJIJYqqJzcegm3CxSO4h06qZ3uDgW3w8ej9_weLw3SXElrjwB_kJg-swAz-MYB_fVP4jHcvmXxW-X31aJ6k73Q-tr5cnDXVJZTtMoKbPs_cBa92PcxEnCBJ1SsmzFOAr9VlpywoCte2EcJKyLPWu1mZasJGrvkeQhSR6R5O7AiimpvCbysqYJECq6yvOaaZgQIE6ReEM3ZQlVOGTK0ORltfdjZEkSdQNAiHQJGBJSDFip6DpSRUNRFQVJOqfpmtQ7uWeHKrpqQN2AUNAMTRVNvjswOqOupst8n8LY38AnA9l-xnoUJukzKjNjgPVd6kzFvKEmPBdiz0YKIyFsM5C3bcZ2eZ4BHPIAFoEgifYBRYcRbvnuYYY8zgwDqjw0lMsTl4hx4jRD7gz26qW-f9z7RL9Tn_64-GX8_XXiYJBV51bWOq1bSzP29Ea7eGceuKo8JwZsI8Li_A2cWI0FVujUlAUOTEllbpsmt2l6n84OUXmiQOlV7hdNPj5H7Gf_f6jD82R3mMtlndCOrZbru2MTHGe7CCCBQTIGDORskbFtGTHAdqDgIAthZHWHYY52mpYfJGOTmwXfradhA7cK5c1CO0jqjtNXa1ZzFSeF8t1CL2rh3tbW1oORM7l_HiFOLxy9eHXy-9Hzn9eOR6_UrGrnqrbeuA2XikUnmk1qi8XZxZuNtoDnKpEcgXRaEWqRHBfVqdd54g81&mkt=en-US&hosted=0&device_platform=Windows+10	false		unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/js/ConvergedLogin_PCore_T2EBBtMmyv072RjbQwNpoQ2.js	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/converged.v2.login.min_9oft0ybq1qhuafkqh5wryq2.css	false	• Avira URL Cloud: safe	unknown
http://https://jmawireless-my.sharepoint.com/	false	• Avira URL Cloud: safe	unknown
http://https://login.microsoftonline.com/fd4efb89-68eb-42bb-bd22-018f0e50365b/oauth2/authorize?client%5Fid=00000003%2D0000%2D0ff1%2Dce00%2D000000000000&response%5Fmode=form%5Fpost&response%5Ftype=code%20id%5Ftoken&resource=00000003%2D0000%2D0ff1%2Dce00%2D000000000000&scope=openid&nonce=E6A2B527BB3449CA22BEDE4081962DCE768F18E74E27A196%2D7665CD0448C60D689D4FFCC8A5D9A9986C1BCB6B6B79CA8FCAD4CD443BDBA5E2&redirect%5Furi=https%3A%2F%2Fjmawireless%2Dmy%2Esharepoint%2Ecom%2F%5Fforms%2Fdefault%2Easpx&state=OD0w&claims=%7B%22id%5Ftoken%22%3A%7B%22xms%5Fcc%22%3A%7B%22values%22%3A%5B%22CP1%22%5D%7D%7D%7D&wsucxt=1&cobrandid=11bd8083%2D87e0%2D41b5%2Dbb78%2D0bc43c8a8e8a&client%2Drequest%2Did=23e42ba1%2D50b5%2D5000%2Da2da%2Dbc6ed7468b83	false		unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/js/asyncchunk/convergedlogin_pcustomizationloader_8e14dcf0e3ff5580d170.js	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/images/marching_ants_986f40b5a9dc7d39ef8396797f61b323.gif	false	• URL Reputation: safe	unknown
http://https://jmawireless-my.sharepoint.com/_layouts/15/Authenticate.aspx?Source=%2F	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://aadcdn.msftauthimages.net/dbd5a2dd-lfa6jvlreimgywhhs-c8kmaqnihskpfu3l8mv5xcc9i/logintenantbranding/0/bannerlogo?ts=637951424196423663	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/images/marching_ants_white_8257b0707cbe1d0bd2661b80068676fe.gif	false	• URL Reputation: safe	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/js/BssoInterrupt_Core_RY3pVDLvjU_KKLtTKxjDFA2.js	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/js/asyncchunk/convergedlogin_pfetchsessionsprogress_7c1aa7609345f99e4914.js	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	false	• URL Reputation: safe	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/images/signin-options_3e3f6b73c3f310c31d2c4d131a8ab8c6.svg	false	• URL Reputation: safe	unknown
http://https://jmawireless-my.sharepoint.com/_forms/default.aspx?ReturnUrl=%2f_layouts%2f15%2fAuthenticate.aspx%3fSource%3d%252F&Source=cookie	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/images/picker_account_aad_a8332c62695d74843a11daf39a74e552.svg	false	• URL Reputation: safe	unknown
http://https://login.microsoftonline.com/fd4efb89-68eb-42bb-bd22-018f0e50365b/oauth2/authorize?client%5Fid=00000003%2D0000%2D0ff1%2Dce00%2D000000000000&response%5Fmode=form%5Fpost&response%5Ftype=code%20id%5Ftoken&resource=00000003%2D0000%2D0ff1%2Dce00%2D000000000000&scope=openid&nonce=E6A2B527BB3449CA22BEDE4081962DCE768F18E74E27A196%2D7665CD0448C60D689D4FFCC8A5D9A9986C1BCB6B6B79CA8FCAD4CD443BDBA5E2&redirect%5Furi=https%3A%2F%2Fjmawireless%2Dmy%2Esharepoint%2Ecom%2F%5Fforms%2Fdefault%2Easpx&state=OD0w&claims=%7B%22id%5Ftoken%22%3A%7B%22xms%5Fcc%22%3A%7B%22values%22%3A%5B%22CP1%22%5D%7D%7D%7D&wsucxt=1&cobrandid=11bd8083%2D87e0%2D41b5%2Dbb78%2D0bc43c8a8e8a&client%2Drequest%2Did=23e42ba1%2D50b5%2D5000%2Da2da%2Dbc6ed7468b83&sso_reload=true	false		unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/watsonsupportwithjquery.3.5.min_dc940oomzau4rsu8qesnvg2.js	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://knockoutjs.com/	chromecache_195.2.dr, chromecache_204.2.dr	false	• URL Reputation: safe	unknown
http://https://github.com/douglascrockford/JSON-js	chromecache_190.2.dr, chromecache_177.2.dr, chromecache_154.2.dr, chromecache_174.2.dr, chromecache_164.2.dr, chromecache_195.2.dr, chromecache_204.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://login.windows-ppe.net	chromecache_145.2.dr	false	• URL Reputation: safe	unknown
http://gsgd.co.uk/sandbox/jquery/easing/	chromecache_165.2.dr	false	• URL Reputation: safe	unknown
http://https://login.microsoftonline.com	chromecache_145.2.dr	false	• URL Reputation: safe	unknown
http://www.opensource.org/licenses/mit-license.php)	chromecache_195.2.dr, chromecache_204.2.dr	false	• URL Reputation: safe	unknown
http://feross.org	chromecache_164.2.dr	false	• URL Reputation: safe	unknown
http://https://account.live.com/resetpassword.aspx	chromecache_169.2.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.107.136.10	dual-spo-0005.spo-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
13.107.246.67	part-0039.t-0009.t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.250.185.164	www.google.com	United States		15169	GOOGLEUS	false
13.107.213.60	part-0032.t-0009.t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
13.107.226.67	part-0039.t-0009.fb-t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
152.199.23.37	cs1100.wpc.omegacdn.net	United States		15133	EDGECASTUS	false

Private

IP
192.168.2.4
192.168.2.5

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1447354
Start date and time:	2024-05-24 21:29:39 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 3m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://jmawireless-my.sharepoint.com
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	8

Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean2.win@22/108@28/9
EGA Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SIHClient.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 173.194.76.84, 216.58.212.174, 142.250.185.163, 34.104.35.123, 20.190.160.17, 40.126.32.74, 20.190.160.22, 40.126.32.72, 40.126.32.134, 40.126.32.133, 40.126.32.136, 40.126.32.76, 2.19.126.200, 2.19.126.199, 40.126.32.138, 20.190.160.14, 40.126.32.140, 20.190.160.20, 20.114.59.183, 2.19.126.137, 2.19.126.151, 192.229.221.95, 20.190.159.71, 40.126.31.67, 20.190.159.2, 40.126.31.69, 20.190.159.4, 20.190.159.64, 20.190.159.0, 40.126.31.73, 20.3.187.198, 172.217.18.106, 142.250.185.74, 142.250.185.138, 142.250.186.42, 142.250.186.138, 172.217.23.106, 142.250.185.202, 142.250.181.234, 216.58.206.42, 142.250.185.234, 142.250.185.106, 142.250.186.74, 142.250.184.234, 142.250.185.170, 216.58.212.170, 172.217.16.138, 20.242.39.171, 40.126.32.129, 40.126.32.6, 40.126.32.131, 40.126.32.66, 152.199.19.160, 20.190.177.0, 172.217.18.3, 95.101.54.121, 95.101.54.113
- Excluded domains from analysis (whitelisted): azurefd-t-fb-prod.trafficmanager.net, slscr.update.microsoft.com, na.privatelink.msidentity.com, clientservices.googleapis.com, a767.dspw65.akamai.net, ak.privatelink.msidentity.com, clients2.google.com, ocsp.digicert.com, login.live.com, update.googleapis.com, wu-b-net.trafficmanager.net, www.ppev6tm.aadg.trafficmanager.net, www.ppev6tm.aadg.akadns.net, fs.microsoft.com, content-autofill.googleapis.com, aadcdnoriginwus2.azureedge.net, aadcdn-msft.azureedge.net, aadcdn-msft.afd.azureedge.net, aadcdn.msauth.net, edgedl.me.gvt1.com, nel.measure.office.net.edgesuite.net, www.tm.f.prd.aadg.trafficmanager.net, aadcdnoriginwus2.afd.azureedge.net, clients.l.google.com, ppe.v6.aadg.privatelink.msidentity.com, 192203-ipv4v6e.farm.dprodmgd105.sharepointonline.com.akadns.net, www.tm.lg.prod.aadmsa.trafficmanager.net, a1894.dscb.akamai.net, mscomajax.vo.msecnd.net, ocsp.edge.digicert.com, glb.cws.prod.dcat.dsp.trafficmanager.net, sls.update.microsoft.com, login.mso.msidentity
- HTTPS proxy raw data packets have been limited to 10 per session. Please view the PCAPs for the complete data.
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtSetInformationFile calls found.
- VT rate limit hit for: https://jmawireless-my.sharepoint.com

Simulations

Behavior and APIs

No simulations

LLM Input / Output

Input	Output

URL: https://login.microsoftonline.com/fd4efb89-68eb-42bb-bd22-018f0e50365b/oauth2/authorize?client%5Fid=00000003%2D0000%2D0ff1%2Dce00%2D000000000000&response%5Fmode=form%5Fpost&response%5Ftype=code%20id%5Ftoken&resource=00000003%2D0000%2D0ff1%2Dce00%2D00 Model: gpt-4o	```json
	{
	"riskscore": 1,
	"reasons": "The JavaScript code appears to be part of a legitimate authentication flow, likely related to Microsoft Azure AD or Office 365 services. The URLs and parameters are consistent with OAuth2 authorization processes. No obvious malicious patterns detected."
	}

Input	Output
//<![CDATA[$Config={"iMaxStackForKnockoutAsyncComponents":10000,"fShowButtons":true,"urlCdn":"https://aadcdn.msftauth.net/shared/1.0/","urlDefaultFavicon":"https://aadcdn.msftauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico","urlPost":"/fd4efb89-68eb-42bb-bd22-018f0e50365b/oauth2/authorize?client_id=00000003-0000-0ff1-ce00-000000000000\u0026response_mode=form_post\u0026response_type=code+id_token\u0026resource=00000003-0000-0ff1-ce00-000000000000\u0026scope=openid\u0026nonce=E6A2B527BB3449CA22BEDE4081962DCE768F18E74E27A196-7665CD0448C60D689D4FFCC8A5D9A9986C1BCB6B6B79CA8FCAD4CD443BDBA5E2\u0026redirect_uri=https%3a%2f%2fjmawireless-my.sharepoint.com%2f_forms%2fdefault.aspx\u0026state=OD0w\u0026claims=%7b%22id_token%22%3a%7b%22xms_cc%22%3a%7b%22values%22%3a%5b%22CP1%22%5d%7d%7d%7d%7d\u0026wsucxt=1\u0026cobrandid=11bd8083-87e0-41b5-bb78-0bc43c8a8e8a\u0026client-request-id=23e42ba1-50b5-5000-a2da-bc6ed7468b83\u0026sso_reload=True","iPawnIcon":0,"sPOST_Username":"","sFTName":"flowToken","dynamicTenantBranding":null,"staticTenantBranding":null,"oAppCobranding":{},"iBackgroundImage":2,"fApplicationInsightsEnabled":false,"iApplicationInsightsEnabledPercentage":0,"urlSetDebugMode":"https://login.microsoftonline.com/common/debugmode","fEnableCssAnimation":true,"fAllowGrayOutLightBox":true,"fIsRemoteNGCSupported":true,"desktopSsoConfig":{"isEdgeAnaheimAllowed":true,"iwaEndpointUrlFormat":"https://autologon.microsoftazuread-sso.com/{0}/winauth/sso?client-request-id=23e42ba1-50b5-5000-a2da-bc6ed7468b83","iwaSsoProbeUrlFormat":"https://autologon.microsoftazuread-sso.com/{0}/winauth/ssoprobe?client-request-id=23e42ba1-50b5-5000-a2da-bc6ed7468b83","iwaIFrameUrlFormat":"https://autologon.microsoftazuread-sso.com/{0}/winauth/iframe?client-request-id=23e42ba1-50b5-5000-a2da-bc6ed7468b83\u0026isAdalRequest=False","iwaRequestTimeoutInMs":10000,"startDesktopSsoOnPageLoad":false,"progressAnimationTimeout":10000,"isEdgeAllowed":false,"minDssoEdgeVersion":"17","isSafariAllowed":true,"redirectUri":"","isIEAllowedForSsoProbe":true,"edgeRedirectUri":"https://autologon.microsoftazuread-sso.com/common/winauth/sso/edgeredirect?client-request-id=23e42ba1-50b5-5000-a2da-bc6ed7468b83\u0026origin=login.microsoftonline.com\u0026is_redirected=1","isFlowTokenPassedInEdge":true},"iSessionPullType":2,"fUseSameSite":true,"isGlobalTenant":true,"uiflavor":1001,"fOfflineAccountVisible":false,"fEnableUserStateFix":true,"fShowAccessPassPeek":true,"fUpdateSessionPollingLogic":true,"fEnableShowPickerCredObservable":true,"fFetchSessionsSkipDsso":true,"fUseNonMicrosoftDefaultBrandingForCiam":true,"fRemoveCustomCss":true,"fFixUICrashForApiRequestHandler":true,"fShowUpdatedKoreanPrivacyFooter":true,"fUsePostCssHotfix":true,"fUseHighContrastOverrides":true,"fFixUserFlowBranding":true,"scid":1013,"hpgact":1800,"hpgid":6,"apiCanary":"PAQABDgEAAADnfolhJpSnRYB1SVj-Hgd8cDKMZrAzkbQe0zujRlWmU8qURPd3D1iX_G1lfRi2nMl_DEJH2nnQzsEgMpGPNqdIfjL9Kbe-IZRYOOC7dXhUpmOH2iNOdweuWBuL6HQaabHuFdajPb6	

URL: https://login.microsoftonline.com/fd4efb89-68eb-42bb-bd22-018f0e50365b/oauth2/authorize?client%5Fid=00000003%2D0000%2D0ff1%2Dce00%2D000000000000&response%5Fmode=form%5Fpost&response%5Ftype=code%20id%5Ftoken&resource=00000003%2D0000%2D0ff1%2Dce00%2D00 Model: gpt-4o
 	
//<![CDATA[
!function(t,e){!function(){var n=e.getElementsByTagName("head")[0];n&&n.addEventListener&&(n.addEventListener("error",function(e){null!==e.target&&"cdn"===e.target.getAttribute("data-loader")&&t.$Loader.OnError(e.target)},!0),n.addEventListener("load",function(e){null!==e.target&&"cdn"===e.target.getAttribute("data-loader")&&t.$Loader.OnSuccess(e.target)},!0))}()}(window,document);
//
	``json
	{
	"riskscore": 1,
	"reasons": "The provided JavaScript code appears to be handling error and success events for loading resources from a CDN (Content Delivery Network). There is no indication of malicious activity such as data exfiltration, credential stealing, or unauthorized access. The code is likely part of a legitimate resource loading mechanism."
	}

URL: https://login.microsoftonline.com/fd4efb89-68eb-42bb-bd22-018f0e50365b/oauth2/authorize?client%5Fid=00000003%2D0000%2D0ff1%2Dce00%2D000000000000&response%5Fmode=form%5Fpost&response%5Ftype=code%20id%5Ftoken&resource=00000003%2D0000%2D0ff1%2Dce00%2D00 Model: gpt-4o
 	
//<![CDATA[
!function(){var e=window,o=e.document,i=e.$Config||{};if(e.self===e.top){o&&o.body&&(o.body.style.display="block")}else if(!i.allowFrame){var s=e.self.location.href,l=s.indexOf("#"),n=-1!==l,t=s.indexOf("?"),f=n?l:s.length,d=-1===t||n&&t>l?"?":"&";s=s.substr(0,f)+d+"iframe-request-id="+i.sessionId+s.substr(f),e.top.location=s}}();
//
	``json
	{
	"riskscore": 2,
	"reasons": "The script checks if the current window is the top window and redirects if it is not. This behavior is often used to prevent clickjacking but can also be used for malicious purposes such as phishing. However, without additional context or more suspicious behavior, the risk is relatively low."
	}

URL: https://passwordreset.microsoftonline.com/?ru=https%3a%2f%2flogin.microsoftonline.com%2ffd4efb89-68eb-42bb-bd22-018f0e50365b%2freprocess%3fctx%3drQQIARAAnVE_aNRgHE2aa-ydrT3q4ljOTj1z-ZJ8Sb4cdMi_04ras3-gnsiRP1_aeJdLmqTtXUsXdRAE6eyidnDoJlJYqqJzcegm3CxSO Model: gpt-4o	```json
	{
	"riskscore": 2,
	"reasons": "The JavaScript code primarily handles AJAX requests to the server for captcha results and tenant branding information. It does not contain any obvious malicious behavior such as credential stealing or unauthorized data access. However, it does interact with server-side endpoints, which could potentially be exploited if the server-side code is not properly secured. The risk is minimal but not zero."
	}

Input	Output

var BANNER_LOGO_URL_KEY = "BannerLogoUrl";
var TENANT_BRAND_NAME_KEY = "TenantBrandName";
 	
function SendCaptchaErrorToServer(result)
{
try
{
$.ajax({
type: "POST",
url: "Default.aspx/ReportCaptchaResult",
contentType: "application/json; charset=utf-8",
dataType: "json",
data: JSON.stringify({
captchaResult: result
}),
success: function (response)
{
},
error: function (response)
{
}
});
}
catch (error)
{
 	
}
}
function UpdateTenantBrandingBannerLogo()
{
try
{
var orgIdTenantDomain = jQuery.trim($('#OrgIdTenantDomain').val());
var orgIdUserName = jQuery.trim($('#OrgIdUserName').val());
var NameCoexistenceAccountValue = jQuery.trim($('#NameCoexistenceAccount').val()
);
var localAccountRequest = false;
 	
if (NameCoexistenceAccountValue == "1")
{
localAccountRequest = true;
}
 	
if (LogoHasBeenPreviouslyLoaded())
{
UpdateLogo(localAccountRequest);
}
else if (orgIdTenantDomain.length > 0 || orgIdUserName.length > 0)
{
$.ajax({
type: "POST",
url: "Default.aspx/GetBrandingInfo",
data: JSON.stringify({
tenantDomain: orgIdTenantDomain,
userName: orgIdUserName,
isLocalAccount: localAccountRequest
}),
contentType: "application/json; charset=utf-8",
dataType: "json",
success: function (response)
{
if (response.d && response.d.length > 0)
{
var tenantInfo = JSON.parse(response.d);
 	
if (tenantInfo.BannerLogoUrl && tenantInfo.TenantBrandName)
{
SetBannerLogoUrl(tenantInfo.BannerLogoUrl);
SetTenantBrandName(tenantInfo.TenantBrandName);
} else	

URL: https://passwordreset.microsoftonline.com/?ru=https%3a%2f%2flogin.microsoftonline.com%2ffd4efb89-68eb-42bb-bd22-018f0e50365b%2freprocess%3fctx%3drQQIARAAnVE_aNRgHE2aa-ydrT3q4ljOTj1z-ZJ8Sb4cdMi_04ras3-gnsiRP1_aeJdLmqTtXUsXdRAE6eyidnDoJlJYqqJzcegm3CxSO Model: gpt-4o
 	
//<![CDATA[
Sys.WebForms.PageRequestManager._initialize('ctl00$ScriptManagerMain', 'form1', ['tctl00$UpdatePanelLogo','UpdatePanelLogo','tctl00$ContentPlaceholderMainContent$UpdatePanelMain','ContentPlaceholderMainContent_UpdatePanelMain'], [], [], 60, 'ctl00');
//
	``json
	{
	"riskscore": 0,
	"reasons": "The provided JavaScript code is related to the initialization of ASP.NET AJAX components and does not contain any malicious elements. It is standard code for managing partial page updates in ASP.NET applications."
	}

Input	Output

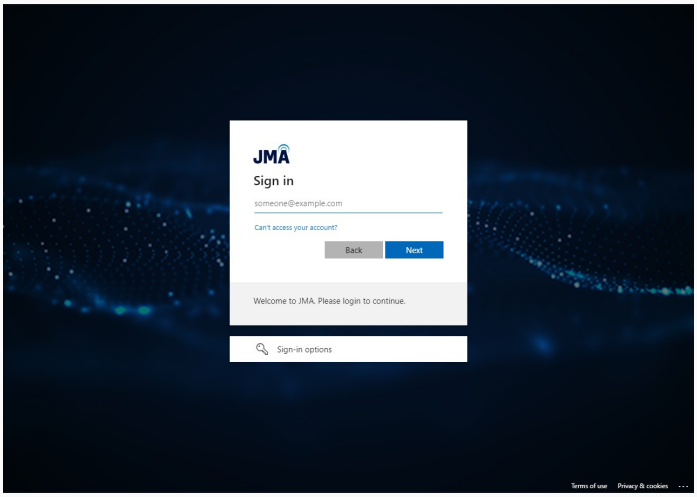
URL: https://passwordreset.microsoftonline.com/?ru=https%3a%2f%2flogin.microsoftonline.com%2ffd4efb89-68eb-42bb-bd22-018f0e50365b%2freprocess%3fctx%3drQQIARAAnVE_aNRgHE2aa-ydrT3q4ljOTj1z-ZJ8Sb4cdMi_04ras3-gnsiRP1_aeJdLmqTtXUsXdRAE6eyidnDoJlJYqqJzcegm3CxSO Model: gpt-4o
 	
//<![CDATA[
var Page_Validators = new Array(document.getElementById("ContentPlaceholderMainContent_RequiredFieldValidatorUserIdentifier"), document.getElementById("ContentPlaceholderMainContent_RegularExpressionValidatorUserIdentifier"), document.getElementById("ContentPlaceholderMainContent_RegularExpressionNonOrgIDDomains"));
//
	``json
	{
	"riskscore": 0,
	"reasons": "The provided JavaScript code is related to form validation using client-side validators. It does not exhibit any malicious behavior such as data exfiltration, credential stealing, or unauthorized access. It appears to be part of a legitimate form validation process."
	}

URL: https://passwordreset.microsoftonline.com/?ru=https%3a%2f%2flogin.microsoftonline.com%2ffd4efb89-68eb-42bb-bd22-018f0e50365b%2freprocess%3fctx%3drQQIARAAnVE_aNRgHE2aa-ydrT3q4ljOTj1z-ZJ8Sb4cdMi_04ras3-gnsiRP1_aeJdLmqTtXUsXdRAE6eyidnDoJlJYqqJzcegm3CxSO Model: gpt-4o
 	
//<![CDATA[
var theForm = document.forms['form1'];
if (!theForm) {
theForm = document.form1;
}
function __doPostBack(eventTarget, eventArgument) {
if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
theForm.__EVENTTARGET.value = eventTarget;
theForm.__EVENTARGUMENT.value = eventArgument;
theForm.submit();
}
}
//
	``json
	{
	"riskscore": 1,
	"reasons": "The provided JavaScript code appears to be standard form handling code, commonly used in web applications to manage form submissions. It does not exhibit any obvious malicious behavior such as data exfiltration, unauthorized access, or manipulation of user data. The code simply sets form values and submits the form. Therefore, it is considered low risk."
	}

URL: https://passwordreset.microsoftonline.com/?ru=https%3a%2f%2flogin.microsoftonline.com%2ffd4efb89-68eb-42bb-bd22-018f0e50365b%2freprocess%3fctx%3drQQIARAAnVE_aNRgHE2aa-ydrT3q4ljOTj1z-ZJ8Sb4cdMi_04ras3-gnsiRP1_aeJdLmqTtXUsXdRAE6eyidnDoJlJYqqJzcegm3CxSO Model: gpt-4o	```json
	{
	"riskscore": 1,
	"reasons": "The provided JavaScript code appears to be related to CAPTCHA functionality, which is a common feature for preventing automated access to web services. The code includes elements for toggling between visual and audio CAPTCHA challenges and handling user interactions. There are no obvious signs of malicious behavior such as data exfiltration, obfuscation, or unauthorized access to sensitive information. The risk score is low, but further context and a full review of the entire codebase would be necessary for a comprehensive security assessment."
	}

Input	Output

var repMapService = {
_currentViewNameId: '#' + 'ContentPlaceholderMainContent_CurrentViewName',
_challengeTypeVisual: 'Visual',
_challengeTypeAudio: 'Audio',
_challengeApiUrl: 'Default.aspx/GetCaptchaChallenge',
_challengeApiMethod: 'POST',
_challengeApiContentType: 'application/json; charset=utf-8',
_challengeLoadingId: '#RepMapChallengeLoading',
_audioIconId: '#' + 'ContentPlaceholderMainContent_RepMapChallengeTypeAudioIcon',
_visualIconId: '#' + 'ContentPlaceholderMainContent_RepMapChallengeTypeVisualIcon',
_repMapCaptchaRootContentId: '#' + 'ContentPlaceholderMainContent_RepMapCaptcha Content',
_visualChallengeElementId: '#RepMapVisualChallenge',
_audioChallengeElementId: '#RepMapAudioChallenge',
_base64VisualPrefix: ' ',
_base64AudioPrefix: 'data:audio/mp3;base64, ',
_audioPlayControlId: '#RepMapAudioPlayControl',
_challengeIdInputId: '#RepMapChallengeId',
_challengeTypeInputId: '#RepMapChallengeType',
_challengeAzureRegionInputId: '#RepMapChallengeAzureRegion',
_getCaptchaErrorMsgId: '#GetCaptchaError',
_toggleChallengeTypeControlId: '#toggleChallengeTypeControl',
_toggleChallengeTypeControlTooltip: '#toggleChallengeTypeControl .tooltip',
_currentChallenge: {
challengeType: 'Visual',
challengeId: ''
},
toggleRepMapServiceChallengeType: function (clickEvent) {
clickEvent.preventDefault(); // Preventing navigation to href=""
var tooltipText = '';
 	
if (this._currentChallenge.challengeType === this._challengeTypeVisual) {
this._currentChallenge.challengeType = this._challengeTypeAudio;
$(this._audioIconId).hide();
$(this._visualChallengeElementId).hide();
$(this._visualIconId).show();
tooltipText = "Use picture mode";
} else {
this._currentChallenge.challengeType = this._challengeTypeVisual;
$(this._audioIconId).show();
$(this._visualChallengeElementId).show();
$(this._visualIconId).hide();
$(this._audioPlayControlId).hide();
tooltipText = "Use audio mode";
}
 	
$(this._toggleChallengeTypeControlId).attr('aria-label', tooltipText);
$(this._toggleChallengeTypeControlTooltip).text(tooltipText);
 	
$(this._visualChallengeElementId).attr("src", '');
$(this._audioChallengeElement	

URL: https://login.microsoftonline.com/fd4efb89-68eb-42bb-bd22-018f0e50365b/oauth2/authorize?client%5Fid=00000003%2D0000%2D0ff1%2Dce00%2D000000000000&response%5Fmode=form%5Fpost&response%5Ftype=code%20id%5Ftoken&resource=00000003%2D0000%2D0ff1%2Dce00%2D0000000 Model: gpt-4o
 
 	
	``json
	{
	"phishing_score": 2,
	"brands": "Microsoft",
	"phishing": false,
	"suspicious_domain": false,
	"has_loginform": true,
	"has_captcha": false,
	"setechniques": false,
	"reasons": "The URL 'https://login.microsoftonline.com' is a legitimate Microsoft domain used for authentication. The login page design matches Microsoft's branding and style. There are no obvious signs of social engineering techniques or suspicious elements in the URL or the image."
	}

Input	Output

URL: https://passwordreset.microsoftonline.com/?ru=https%3a%2f%2flogin.microsoftonline.com%2ffd4efb89-68eb-42bb-bd22-018f0e50365b%2freprocess%3fctx%3drQQIARAAnVE_aNRgHE2aa-ydrT3q4ljOTj1z-ZJ8Sb4cdMi_04ras3-gnsiRP1_aeJdLmqTtXUsXdRAE6eyidnDoJlJYqqJzcegm3CxSO Model: gpt-4o
 	
//<![CDATA[
$addHandler(window.document.documentElement, 'mouseup', Button.MouseUp); Sys.Application.add_init(Button.ResizeButtons);
var Page_ValidationActive = false;
if (typeof(ValidatorOnLoad) == "function") {
    ValidatorOnLoad();
}
 	
function ValidatorOnSubmit() {
    if (Page_ValidationActive) {
        return ValidatorCommonOnSubmit();
    }
    else {
        return true;
    }
}
        WebForm_AutoFocus('ContentPlaceholderMainContent_TextBoxUserIdentifier');
document.getElementById('ContentPlaceholderMainContent_RequiredFieldValidatorUserIdentifier').dispose = function() {
    Array.remove(Page_Validators, document.getElementById('ContentPlaceholderMainContent_RequiredFieldValidatorUserIdentifier'));
}
 	
document.getElementById('ContentPlaceholderMainContent_RegularExpressionValidatorUserIdentifier').dispose = function() {
    Array.remove(Page_Validators, document.getElementById('ContentPlaceholderMainContent_RegularExpressionValidatorUserIdentifier'));
}
 	
document.getElementById('ContentPlaceholderMainContent_RegularExpressionNonOrgIDDomains').dispose = function() {
    Array.remove(Page_Validators, document.getElementById('ContentPlaceholderMainContent_RegularExpressionNonOrgIDDomains'));
}
Button.DefaultButton='ContentPlaceholderMainContent_ButtonNext';$addHandler(window.document.documentElement, 'keyup', Button.DefaultButtonKeyUpHandler);$addHandler(window.document.documentElement, 'keydown', Button.DefaultButtonKeyDownHandler);Button.AttachDefaultButtonHandlers();Sys.Application.add_init(function() {
    $create(Sys.UI._UpdateProgress, {"associatedUpdatePanelId":"ContentPlaceholderMainContent_UpdatePanelMain","displayAfter":0,"dynamicLayout":false}, null, null, $get("ContentPlaceholderMainContent_UpdateProgress1"));
});
//
	``json
	{
	  "riskscore": 1,
	  "reasons": "The provided JavaScript code appears to be related to form validation and user interface interactions, such as handling button events and validators. There are no obvious signs of malicious activity such as data exfiltration, unauthorized access, or harmful operations. The code seems to be part of a legitimate web application. However, without more context or a deeper analysis, a minimal risk score is assigned."
	}

URL: https://passwordreset.microsoftonline.com/?ru=https%3a%2f%2flogin.microsoftonline.com%2ffd4efb89-68eb-42bb-bd22-018f0e50365b%2freprocess%3fctx%3drQQIARAAnVE_aNRgHE2aa-ydrT3q4ljOTj1z-ZJ8Sb4cdMi_04ras3-gnsiRP1_aeJdLmqTtXUsXdRAE6eyidnDoJlJYqqJzcegm3CxSO Model: gpt-4o	```json
	{
	  "riskscore": 2,
	  "reasons": "The code includes functions related to password handling and client-side validation, which could be a target for malicious activities. However, there is no direct evidence of malicious intent in the provided code. The code appears to be part of a legitimate web application's user interface handling."
	}

Input	Output

function pageLoad() {
CheckWorkflowConsistency();
ShowPasswordPopup();
InitializePasswordStrengthMeterAndHelpContainerOnLoad();
repMapService.showRepMapServiceChallenge();
}
 	
var notifyAdministratorClicked = 0;
 	
function ButtonNextClick(sender) {
if ($get('Buttons').style.display == 'none') {
sender.disabled = 'true';
return false;
}
 	
captchaError = $get('ContentPlaceholderMainContent_LabelCaptchaError');
SetDisplayStateNone(captchaError);
 	
// do client side validation
if (typeof (Page_ClientValidate) == 'function') {
if (Page_ClientValidate() == false) {
// clear error strings that are set server side to show client side validation errors
var userIdErrorLabel = $get('ContentPlaceholderMainContent_UserIdErrorLabel');
if (userIdErrorLabel) {
userIdErrorLabel.style.display = 'none';
}
var labelCaptchaError = $get('ContentPlaceholderMainContent_LabelCaptchaError');
if (labelCaptchaError) {
labelCaptchaError.style.display = 'none';
}
var labelSetPasswordErrorMessage = $get('ContentPlaceholderMainContent_Label
SetPasswordErrorMessage');
if (labelSetPasswordErrorMessage) {
labelSetPasswordErrorMessage.style.display = 'none';
}
return false;
}
}
// hide buttons
$get('Buttons').style.display = 'none';
}
 	
function ButtonCancelClick() {
$get('Buttons').style.display = 'none';
}
 	
function ButtonContactAdministratorClick(button) {
if (notifyAdministratorClicked != 0) {
return false;
}
else {
notifyAdministratorClicked = notifyAdministratorClicked + 1;
}
}
 	
function ButtonContactAdministrator_ClientClick(button) {
var hiddenAnchor = $get('ContentPlaceholderMainContent_ContactAdmin_Hidden_Ancho
r');
 	
if (hiddenAnchor && hiddenAnchor.click) {
hiddenAnchor.click();
return false;
}
ButtonContactAdministratorClick(button);
}
 	
// Toggles style.display of given element between 'none' and 'block'
function ToggleDisplayState(elementId) {
var element = $get(elementId);
if (element) {
if (element.style.display == '	

URL: https://passwordreset.microsoftonline.com/?ru=https%3a%2f%2flogin.microsoftonline.com%2ffd4efb89-68eb-42bb-bd22-018f0e50365b%2freprocess%3fctx%3drQQIARAAnVE_aNRgHE2aa-ydrT3q4ljOTj1z-ZJ8Sb4cdMi_04ras3-gnsiRP1_aeJdLmqTtXUsXdRAE6eyidnDoJlJYqqJzcegm3CxSO Model: gpt-4o	```json
	{
	"riskscore": 1,
	"reasons": "The provided JavaScript code appears to be focused on form validation, specifically for email addresses. It includes validation for required fields and regular expressions to ensure the email format is correct. There are no indications of malicious activity such as data exfiltration, obfuscation, or unauthorized access to user information. The code does not perform any actions beyond form validation and error messaging. Therefore, it poses minimal risk."
	}

Input	Output

//<![CDATA[
var ContentPlaceholderMainContent_RequiredFieldValidatorUserIdentifier = document.all ? document.all["ContentPlaceholderMainContent_RequiredFieldValidatorUserIdentifier"] : document.getElementById("ContentPlaceholderMainContent_RequiredFieldValidatorUserIdentifier");
ContentPlaceholderMainContent_RequiredFieldValidatorUserIdentifier.controltovalidate = "ContentPlaceholderMainContent_TextBoxUserIdentifier";
ContentPlaceholderMainContent_RequiredFieldValidatorUserIdentifier.focusOnError = "t";
ContentPlaceholderMainContent_RequiredFieldValidatorUserIdentifier.errormessage = "Please type your email address in the format user@contoso.onmicrosoft.com or user@contoso.com";
ContentPlaceholderMainContent_RequiredFieldValidatorUserIdentifier.display = "Dynamic";
ContentPlaceholderMainContent_RequiredFieldValidatorUserIdentifier.evaluationfunction = "RequiredFieldValidatorEvaluateIsValid";
ContentPlaceholderMainContent_RequiredFieldValidatorUserIdentifier.initialvalue = "";
var ContentPlaceholderMainContent_RegularExpressionValidatorUserIdentifier = document.all ? document.all["ContentPlaceholderMainContent_RegularExpressionValidatorUserIdentifier"] : document.getElementById("ContentPlaceholderMainContent_RegularExpressionValidatorUserIdentifier");
ContentPlaceholderMainContent_RegularExpressionValidatorUserIdentifier.controltovalidate = "ContentPlaceholderMainContent_TextBoxUserIdentifier";
ContentPlaceholderMainContent_RegularExpressionValidatorUserIdentifier.focusOnError = "t";
ContentPlaceholderMainContent_RegularExpressionValidatorUserIdentifier.errormessage = "Please type your email address in the format user@contoso.onmicrosoft.com or user@contoso.com";
ContentPlaceholderMainContent_RegularExpressionValidatorUserIdentifier.display = "Dynamic";
ContentPlaceholderMainContent_RegularExpressionValidatorUserIdentifier.evaluationfunction = "RegularExpressionValidatorEvaluateIsValid";
ContentPlaceholderMainContent_RegularExpressionValidatorUserIdentifier.validationexpression = "^\\s*[a-zA-Z0-9~;&#^\\\\!.\'_%-]+@[a-zA-Z0-9](?!.*\\.\\..*)[a-zA-Z0-9.-]*\\.[a-zA-Z]{2,25}\\s*$";
var ContentPlaceholderMainContent_RegularExpressionNonOrgIDDomains = document.all ? document.all["ContentPlaceholderMainContent_RegularExpressionNonOrgIDDomains"] : document.getElementById("ContentPlaceholderMainContent_RegularExpressionNonOrgIDDomains");
ContentPlaceholderMainContent_RegularExpressionNonOrgIDDomains.controltovalidate = "ContentPlaceholderMainContent_TextBoxUserIdentifier";
ContentPlaceholderMainContent_RegularExpressionNonOrgIDDomains.focusOnError = "t";
ContentPlaceholderMainContent_RegularExpressionNonOrgIDDomains.errormessage = "Microsoft Accounts or personal email addresses dont work here. Make sure you enter your work or school account (e.g. user@contoso.com). If you want to reset a Microsoft Account password, click here.";
ContentPlaceholderMainContent_RegularExpressionNonOrgIDDomains.dis	

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

Chrome Cache Entry: 144

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 192 x 103, 8-bit/color RGBA, non-interlaced

Category:	downloaded
Size (bytes):	8360
Entropy (8bit):	7.923599325221617
Encrypted:	false
SSDEEP:	192:KTdWiPEkbEcxdpJTKabqLc73FEVhLmgez+S1vhXpj5AUqpVL:KdWiPEkEcfr32PLmge6ovhX95kL
MD5:	91821BD2E6B92C98235D686A1EED2143
SHA1:	196B7D9C770638AB60021063E2E49097B081B1B9
SHA-256:	381DCF4936A6D425D97D719E4E4C47A2A6D07A7933F16709AEC9AE383FBFC716
SHA-512:	50D6B7C2B1666BBB1379F289AD61B306BFD8C339244A5050BFFC8C02FE82BC3EF2D542927CF982F4F33E4C6B208D9FAA76E2D1FD1E89EEB66D5CC9541353F29
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msftauthimages.net/dbd5a2dd-lfa6jvlreimgywhhs-c8kmaqnihskpfu3l8mv5xcc9i/logintenantbranding/0/bannerlogo?ts=637951424196423663
Preview:	.PNG.....IHDR.....g.....V.MQ....sRGB.....gAMA.....a.....pHYs...t...t..f.x....tEXtSoftware.Adobe ImageReadyq.e<...&iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 7.1-c000 79.98d7942, 2022/03/21-11:40:59 "> <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 22.5 (Macintosh)" xmpMM:InstanceID="xmp.iid:4F012883FBAE11ECB5C18791D51607AC" xmpMM:DocumentID="xmp.did:4F012884FBAE11ECB5C18791D51607AC"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:4F012881FBAE11ECB5C18791D51607AC" stRef:documentID="xmp.did:4F012882FBAE11ECB5C18791D51607AC"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>...;....IDATx^..|T...O2K.IB....*.....".P.Z.(...-.....E.O[..

Chrome Cache Entry: 145

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text, with very long lines (2345), with CRLF line terminators
Category:	downloaded
Size (bytes):	2347
Entropy (8bit):	5.290031538794594
Encrypted:	false
SSDEEP:	48:gCgF0+kNL5iQ6+GhB+SYWzGuesAFcsGJOzgO6FIEv+sj+M++sx+suse+swsosmC0:gC3Na5+GX+Ti2XsYE2sqAsosushswsoB
MD5:	E86EF8B6111E5FB1D1665BCDC90888C9
SHA1:	994BF7651CB967CD9053056AF2D69ACB74DB7F29
SHA-256:	3410242720DE50B090D07A23AEE2DAD879B31D36F2615732962EC4CFA8A9D458
SHA-512:	2486B491681EE91A9CD1ECC9AA011A3FB34B48358C5D7A4D503A5357BC5CE4CA22999F918D40AC60A3063940D5F326FC7E4E5713D89D5C102DE68824E371B3AB
Malicious:	false
Reputation:	low
URL:	http://https://login.live.com/Me.htm?v=3
Preview:	<script type="text/javascript">!function(n,t){for(var e in t)n[e]=t[e]}(this,function(n){function t(i){if(e[i])return e[i].exports;var s=e[i]={exports:{},id:i,loaded:!1};return n[i].call(s.exports,s,s.exports,t),s.loaded=!0,s.exports}var e={};return t.m=n,t.c=e,t.p="",t(0)}([function(n,t){function e(n){for(var t=g[c],e=0,i=t.length;e<i;++e)if(t[e]===n)return!0;return!1}function i(n){if(!n)return null;for(var t=n+"=",e=document.cookie.split(";"),i=0,s=e.length;i<s;i++){var o=e[i].replace(/^\s*(\w+)\s*=\s*/,"$1=").replace(/(\s+$)/,"");if(0===o.indexOf(t))return o.substring(t.length)}return null}function s(n,t,e){if(n)for(var i=n.split(":"),s=null,o=0,a=i.length;o<a;++o){var l=null,c=i[o].split("$");if(0===o&&(s=parseInt(c.shift()),!s))return;var p=c.length;if(p>=1){var f=r(s,c[0]);if(!f||e[f])continue;l={signInName:f,idp:"msa",isSignedIn:!0}}if(p>=3&&(l.firstName=r(s,c[1]),l.lastName=r(s,c[2])),p>=4){var g=c[3],m=g.split("|");l.otherHashedAliases=m}if(p>=5){var h=parseInt(c[4],16);h&&(l.

Chrome Cache Entry: 146

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	379
Entropy (8bit):	4.942805876241154
Encrypted:	false
SSDEEP:	6:tl9mc4slztdbC/yXADQKDTcVEq0FyX4bVGEynbtwag8R+mkbtR1dI1zAmiadc:t4pb8WsQKvkB0wX4gEkbtLv8mkbtvdle
MD5:	2D8F86059BE176833897099EE6DDEDEB
SHA1:	93A2E327027DEED53076E86BFA7D9EEBBF0CC4B9
SHA-256:	34D8DA073F47030EE94B99D84FBE68E3345BD8AAA37EA909FF2DA00238447486
SHA-512:	64D75B1F35180FF61F5BF11D21544454DF016D0854573D75D277FCB933CE845D1436BDC822445B78C627A1FF730B39FC34B72C27D45A39E237F2CCF0876FCA4E
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="48" height="48" viewBox="0 0 48 48"><title>assets</title><circle cx="24" cy="24" r="24" fill="#e6e6e6"/><path d="M13.44,36h1.92a8.64,8.64,0,1,1,17.28,0h1.92a10.573,10.573,0,0,0-6.569-9.771,7.68,7.68,0,1,0-7.982,0A10.573,10.573,0,0,0,13.44,36Zm4.8-16.32A5.76,5.76,0,1,1,24,25.44,5.766,5.766,0,0,1,18.24,19.68Z" fill="#404040"/></svg>

Chrome Cache Entry: 147

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, Unicode text, UTF-8 text, with very long lines (941), with CRLF line terminators
Category:	dropped
Size (bytes):	51589
Entropy (8bit):	4.642771856709614
Encrypted:	false
SSDEEP:	768:3VBsIcaywIR/L5IBRe7RMCb9LlQfWGfAlBRsYXzrSSl:3VjyrRSBRe7eChlQfWGfAlBRsYX6Sl
MD5:	B1357E51586896F14A63743CB9EC163C
SHA1:	91AC0AA31A90D4F10B62E7C6D238AC3F2D2A9E5C
SHA-256:	806BB02EB703D4651546EEB70BC1D82C8D5B7EB72F65D4B5EB28BB311846DAA4
SHA-512:	68B08C89C6282C818FAE0D5F1BCC2CDF0E9BD356AD902CEE46295FC1D0E05D26ADC01202F39532EA985F969C0245236EB0745A8ECEF4DFE77EED3DED8877E399
Malicious:	false
Reputation:	low
Preview:	..<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">..<html xmlns="http://www.w3.org/1999/xhtml" dir="ltr" lang="en-US">..<head><title>...Microsoft Online Password Reset..</title><meta http-equiv="x-ua-compatible" content="IE=9" /><meta http-equiv="Expires" content="0" /><meta http-equiv="Pragma" content="no-cache" /><meta http-equiv="Cache-Control" content="no-store, no-cache" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta name="robots" content="noindex, nofollow, NOODP, NOYDIR" /><meta name="viewport" content="width=device-width, initial-scale=1" /><link id="FavoriteIcon" rel="Shortcut Icon" type="image/x-icon" href="../favicon.ico?v=1342177280" />.... <script src="//ajax.aspnetcdn.com/ajax/jQuery/jquery-3.6.0.min.js" type="text/javascript"></script>.. <script type="text/javascript">window.jQuery || document.write('<script type="text/javascript" src="../js/jquery-3.6.0.min.js">\

Chrome Cache Entry: 148

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 352 x 3
Category:	dropped
Size (bytes):	2672
Entropy (8bit):	6.640973516071413
Encrypted:	false
SSDEEP:	48:ZaOdwduTYPpS9pZy9vDNi1miicsvrJkafMiS+MGQ09DU/X9/4Xp6m5Z9SQcq:4CIuTYPpSTc9vcPZX9/2gzQ/
MD5:	166DE53471265253AB3A456DEFE6DA23
SHA1:	17C6DF4D7CCF1FA2C9EFD716FBAE0FC2C71C8D6D
SHA-256:	A46201581A7C7C667FD42787CD1E9ADF2F6BF809EFB7596E61A03E8DBA9ADA13
SHA-512:	80978C1D262BC225A8BA1758DF546E27B5BE8D84CBCF7E6044910E5E05E04AFFEFEC3C0DA0818145EB8A917E1A8D90F4BAC833B64A1F6DE97AD3D5FC80A02308
Malicious:	false
Reputation:	low
Preview:	GIF89a`.....!..NETSCAPE2.0.....!.....,....`.....6.....P.I.....H....I..:qJ.....k....`BY..L*..&...!.....,....0.....<....[.\K8j.tr.g..!.....,....3.....^;.*..\UK.]\.%.V.c...!.....,....7.....`....lo...[.a..*Rw~i...!.....,....;.....h.....I.G-.[K.,_XA]..'g..!.....,....?.....i.....g....Z.}..)..u...F..!.....,....C.....P..nt^.i....Xq...i..!.....,....F.....{^b....n.y..i...\C.-...!.....,....H.....R...o....h.xV!.z#...!.....,"...L.....r.jY..w~aP(.....[i...!.....,(...N.....r....w.aP.j.')Y..S..!.....,....H.....`.....hew..9`.%z.xVeS..!.....,5...A.....`...\m.Vmtzw.}.d.%...Q..!.....,9...=.....h.....3S..s.-W8m...Q..!.....,A...5.....h.....N...:..!..U..!.....,H.....h....M.x...f.i.4..!.....,O...'.....i...tp.....(..!.....,X.....j...@.x....!.....,].....j..L..3em..!.....,e.....`.....!.....,n.....{i..!..

Chrome Cache Entry: 149

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (61177)
Category:	downloaded
Size (bytes):	113124
Entropy (8bit):	5.28507405223626
Encrypted:	false
SSDEEP:	1536:QpHDgBvguhw+EViazA/PWrF7qvEAFiQcpmchSeC1Jzc6VUWG:xkNhp6VUT
MD5:	F4E7EDD1806AD6A86E69F910879591C9
SHA1:	D39B8F7E60C1D3832296ECED130B6A9EE4CD24D8
SHA-256:	7363ADBB18193C85AC24339AB57B08DF1C8EF875186EDBC85D1CE9184A05A20B
SHA-512:	148CDCBAE4E8DA9EDC4588F422C1C9A0D6DD80F441B1D7C380107F7FE7A750948984EC0581AE61CC56CBE1EC850730A6E373ACECC024E98A914EA2793FBB665C
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/converged.v2.login.min_9oft0ybq1qhuafkqh5wryq2.css
Preview:	/*! Copyright (C) Microsoft Corporation. All rights reserved. *//*!---------- 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 any person

Chrome Cache Entry: 150	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12980
Entropy (8bit):	4.656952280411437
Encrypted:	false
SSDEEP:	384:QjJmcs01WskN59g1+VW1aEV4xvbw94l1R5SUcZEWajJIcjqTqxBojafes0OPUE9h:t4i7l1rSVajJWjs0O8E9h
MD5:	8EDFCD3F7A179CFF6B123DFF50F29770
SHA1:	7A2D9BB4B9F6072AB3049E6421021A5BA0A3DADF
SHA-256:	D0B747C7F7414A08B0D5107832B2F4BB44A9BB4A3AAD28390F58EDE8BBEA6AE1
SHA-512:	169D1C71078DCB1C65B3CBAFBA3379B94718D6C1E472990666430A6B2C0483CC9B27E13820A29D2DCA2364D3CD3F7D2ECDED48B9ACF406BF74CB505489FB903
Malicious:	false
Reputation:	low
URL:	http://https://passwordreset.microsoftonline.com/js/Button.js?v=1342177280
Preview:	.//----------.// Copyright (c) Microsoft Corporation. All rights reserved...//----------....var Button = new Object();....Button.ActiveButton = null;..Button.FocusButton = null;..Button.DefaultButton = null;..Button.CancelButton = null;..Button.ActivatedButtonID = null;..Button.Groups = {};....Button.SetText = function(id, text) {.. var button = document.getElementById(id);.. if (button != null) {.. for (var i = 0; i < button.children.length; i++) {.. var ch = button.children[i];.. if (ch.tagName.toLowerCase() == 'span') {.. ch.innerHTML = text; //// TODO: this causes the text wrapped with an <a> tag to get inserted in Firefox, which needs to get fixed... break;.. }.. }.. }.. var span = document.getElementById(id + '_disabled');.. if (span != null) {.. for (var i = 0; i < span.childr

Chrome Cache Entry: 151	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1378
Entropy (8bit):	4.316299265862323
Encrypted:	false
SSDEEP:	24:t4pb8m3NquUzOqnXmZcU4BC+CaAIA5cAEisx+fUu3fLkY:zoNLUzOeXfU4BJxA5fXUWx
MD5:	F83EBFF69A4A1685E4DC9650CDAB8886
SHA1:	FD21658884945B00157557AE06803DAA6A9F10C6
SHA-256:	7B1669DA90261CDB1483950BB480AD96875F84B09BC48D1055303CE94821BF64
SHA-512:	AA21A03AB84FA0129AFCED8A56E499757A6625C9B24A81EE08F5775B9B542F71BA67EAE817D633CB4E4533A8CF6A0DDA80BD7EE8A90E95AB3D39A77F88073F23
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="48" height="48" viewBox="0 0 48 48"><defs><style>.a{fill:#e6e6e6;}.b{fill:#404040;}</style></defs><circle class="a" cx="24" cy="24" r="24"/><path class="b" d="M32.5,14A1.492,1.492,0,0,1,34,15.5V38.5A1.494,1.494,0,0,1,32.5,40h-17A1.494,1.494,0,0,1,14,38.5v-23A1.494,1.494,0,0,1,15.5,14h4.873l-3-6h2.25l3,6h2.751l3-6h2.25l-3,6ZM32,16H23.623l1.266,2.546A1.13,1.13,0,0,1,25,19a1.009,1.009,0,0,1-1,1,1,1,0,0,1-.534-.149.974.974,0,0,1-.368-.4L21.375,16H16v22h32ZM20,26a3.92,3.92,0,0,1,.312-1.555,4.023,4.023,0,0,1,2.133-2.133,4.041,4.041,0,0,1,3.109,0,4.014,4.014,0,0,1,2.133,2.133A3.886,3.886,0,0,1,28,26a3.937,3.937,0,0,1-.288,1.485,3.987,3.987,0,0,1-.8,1.266A5.7,5.7,0,0,1,28.2,29.7a5.907,5.907,0,0,1,.968,1.251,6.388,6.388,0,0,1,.616,1.461A5.786,5.786,0,0,1,30,34H28a3.877,3.877,0,0,0-.312-1.554,4,4,0,0,0-2.133-2.133,4.011,4.011,0,0,0-3.109,0,4.023,4.023,0,0,0-2.133,2.133A3.912,3.912,0,0,0,20,33.995H18a5.786,5.786,0,0,1,.218-1.586,6.388,6.388,0,0,1,.61

Chrome Cache Entry: 152	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65446), with CRLF line terminators
Category:	downloaded
Size (bytes):	89503
Entropy (8bit):	5.290152941028811
Encrypted:	false
SSDEEP:	1536:ejExXUqJnxDjoXEZxkMV4QYSt0zvDL6gP3h8cApwEIOzVTB/UjPazMdLiX4mQ1vE:eIh8GgP3hujzwbhd3XvSiDQ47GKq
MD5:	0732E3EABBF8AA7CE7F69EEDBD07DFDD
SHA1:	4CD5DDC413B3024D7B56331C0D0D0B2BD933F27F
SHA-256:	CE9D07500AD91EC2B524C270764EC4C9A33E78320D8D374EC400EDE488F6251B
SHA-512:	41D24C426ABCF913BE59917591D906318A547661280036B098A2B1B948BCF9FF14F268B140DB10956730D64A857A61B81034D888ED7F857419DEE6B8D327447C
Malicious:	false
Reputation:	low
URL:	http://https://passwordreset.microsoftonline.com/js/jquery-3.6.0.min.js

Preview:	/*! jQuery v3.6.0 | (c) OpenJS 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(C,e){"use strict";var t=[],r=Object.getPrototypeOf,s=t.slice,g=t.flat?function(e){return t.flat.call(e)}:function(e){return t.concat.apply([],e)},u=t.push,i=t.indexOf,n={},o=n.toString,v=n.hasOwnProperty,a=v.toString,l=a.call(Object),y={},m=function(e){return"function"==typeof e&&"number"!=typeof e.nodeType&&"function"!=typeof e.item},x=function(e){return null!=e&&e===e.window},E=C.document,c={type:!0,src:!0,nonce:!0,noModule:!0};function b(e,t,n){var r,i,o=(n=n||E).createElement("script");if(o.text=e,t)for(r in c)(i=t[r]||t.getAttribute&&t.getAttribute(r))&&o.setAttribute(r,i);n.head.appendChild(o).parentNode.removeChild(o)}func

Chrome Cache Entry: 153	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 60 x 60, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1561
Entropy (8bit):	7.762338770217686
Encrypted:	false
SSDEEP:	48:c/CeK/fE+XoVldlkPdTWbuf173xX964boBdlhLE:ntcx/lksbuf17f64borlK
MD5:	8DC34013E911C5F68FC2BCA0400CB06F
SHA1:	16BAFA91AF100D65C4945F04E0C6E1643B98CF00
SHA-256:	795029D360C3D16233FCE96F1BFF13C261535C0885FAE806CFF766F32D96BCEE
SHA-512:	83ACA42A30BFD629BC1E88D3ED154475E7949C1B154D19E6C9EF1DE825BA7967C0B6DA9EE79E7B420668242CCE5931DF344C97278A254F0A72C3D09EABED6051
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...<...<.....:..r....sBIT....|.d.....pHYs.....S.....tEXtCreation Time.05/06/16...o....tEXtSoftware.Adobe Fireworks CS6.....qIDATh..=l.E.....H..H*.|... ...&.D.).@....&...N....)_.E ...(.p...p(H...Ht... ..0.....i.}s.....{`ss...;.....:...u..."....Az.r.%.9.|....wU.j...o....N4...~....g.u.=`.;..9.7.%....Ad#.....9....~7.....&.a.....`]x^D....&,"..kv.l..K.S+!..#{.xm.;..%.+F<.\..#...bN...2...\.".I..U]..#.dWy$."r.2;Z...w)oD..H..u..M.'.k70.<4aG..`'~.....k31W.2!Ue.A"..j....X..C...dNUd.... .j.\|c."..../..P.MXD.....C`>7Y.K...n.....U..#..^4. ...Uu...Q.);.`9q.53..n.@.....A6.E,6.-d; .....nl.>..."..N7..9\6.....p^a..4aG...3...gUu#..j...2.....f.....^.)...Udo'&..G.C.Z...L).....".t...pCD..n..a.....E....F...o.k.Y+b...[...gT..... ...]. ...V..m.!\..SCwh8w..J^.3N.....\.W.....3.....IP.Da.....-.....@_...i.....r..%..)E.Q...3..M..o.$...`..."....../-/EHIDZ.q.MC.....D.Q.."... ..#.....1...p.x?dKP.=...{u\.

Chrome Cache Entry: 154	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (512)
Category:	downloaded
Size (bytes):	11970
Entropy (8bit):	5.416120131770621
Encrypted:	false
SSDEEP:	192:FPpd9ihiovIZwqsTh8Mi0Yl82YmYZewHe+IkA1niOpVTChGZu3PcXVstaD:ddElyi0u82Y9ZewHPIkA1niOpVmOUPcX
MD5:	39A0EB35CD7799A181D34F4AE1DDB496
SHA1:	E933CA8534BCB6AD79D240316CE23C8B870050D0
SHA-256:	C8CEF105FCAF7CBF3F8682C861045505C24D41CF6686C20C1C03E14031A3DB69
SHA-512:	0AE990F9B57B55C3A8025BBE13C98ECD8A40C38380F9E0EFEF2BE7B418642EB040E4C537E684D2FEF7E04113450CFD4DEFF3414310773177220209991BBF1643
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/frameworksupport.min_oadrnc13magb009k4d20lg2.js
Preview:	/*! --- START OF THIRD PARTY NOTICE ---..This file is based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise. .. * json2.js (2016-05-01). * https://github.com/douglascrockford/JSON-js. * License: Public Domain..Provided for Informational Purposes Only..Public Domain. .NO WARRANTY EXPRESSED OR IMPLIED. USE AT YOUR OWN RISK..--- END OF THIRD PARTY NOTICE --- */."object"!=typeof JSON&&(JSON={}),

Chrome Cache Entry: 155	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 4 icons, 64x64, 32 bits/pixel, 32x32, 32 bits/pixel
Category:	downloaded
Size (bytes):	24038
Entropy (8bit):	5.992474931914016
Encrypted:	false
SSDEEP:	384:cLU4fKWVUvyZk56/1+fZfMj8hTb5nz0bnOWWWWWWWWWWWWWWWWWWWWWWWWqvESs:cLxfKW6yZk8/iZfMjYxnzonm9MaKcuwW
MD5:	877784A5F5808CEFA2B61E73BFCF8EAE
SHA1:	6A0E7EDA2734D7BBBA3CE38D37B347DF001B1DBF
SHA-256:	BE7F0632337BC381D4962125545A5CC3C1E84E2D03DBDB97AB3D79AD78B91B6D
SHA-512:	DABFFC928F7ED2A2D05003DAEF643806BD1CEC6B98E705F7415A82AFE7034F4E1E8A70C5AE69B094A948EEDAB4E8B76DCF72DF881DA092FE4AB76DA0EEFB8C3C
Malicious:	false

Reputation:	low
URL:	http://https://passwordreset.microsoftonline.com/favicon.ico?v=1342177280
Preview:	......@@.... .(@..F... .... .(...n@..... .(....P..... .(....Y..(...@..... .....W.X..~S...W...X...X...X..X..V..p...}..... .....kQ.W*..S$..wK..k..k..k..m..m..p..q..q..r..~.....".....t..s'..^...\...^...._..._...`...a...b...e...M..... .....fF.^...sB...m...v...w...x...x...y...{...{.....%...#..."..".. .....v._..xL...V...X...X...Y...Z...Z...\...`..}N...k#..... .....rO4.Y+...T...k...q...q...p...q...q...u..}...."...$... .....j...S...T...X...Z...Y...Z...[...Z...]..._..{O...o?..... .....

Chrome Cache Entry: 156

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 352 x 3
Category:	downloaded
Size (bytes):	3620
Entropy (8bit):	6.867828878374734
Encrypted:	false
SSDEEP:	48:ZumKaT5ezv47j2/ZiRDlq16x8XvEUcg777shHdpHVGJqFd:Eal647jPDlL8XvEUcg77kVGyd
MD5:	B540A8E518037192E32C4FE58BF2DBAB
SHA1:	3047C1DB97B86F6981E0AD2F96AF40CDF43511AF
SHA-256:	8737D721808655F37B333F08A90185699E7E8B9BDAAA15CDB63C8448B426F95D
SHA-512:	E3612D9E6809EC192F6E2D035290B730871C269A267115E4A5515CADB7E6E14E3DD4290A35ABAA8D14CF1FA3924DC76E11926AC341E0F6F372E9FC5434B546E5
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msftauth.net/shared/1.0/content/images/marching_ants_986f40b5a9dc7d39ef8396797f61b323.gif
Preview:	GIF89a`.....iii!.....!.&Edited with ezgif.com online GIF maker.!..NETSCAPE2.0.....,...`.....6.....P.I.....H....I...:qJ.....k....`BY..L*..&...!.....,...`.....9..i....Q4.....H..j.=.k9-5_.. .....j7..({.....!.....,...`.....9.....trV.....H....`.[.q6.....>.. .CZ.&!.....M...!.....,...`.....8.....:.....H..jJ..U..6_...../.el...q.)...*..!.....,...`.....9....i..l.go.....H..*".U...f....._.....5 .....n..!.....,...`.....:..i...../.....H...5%.kE/5.....In.a..@&3.....J...!.....,...`.....9.....kr.j.....H..*.-.{Im5c.....@&.....!.....,...`.....9.....j..q....H...]..&..\.5.....8..S.....!. .....,...`.....9.....3q.g..5....H...:u.....Al..x.q.....!.....,...`.....9.....\.F....z....H...zX...ov.....h3N.x4.....j..!.....,...`....9.....Q.:.....H....y..^...1.....n.!.F.....E...!.....,.. ..`.....8.....i,.....H....*_.21.I.....%...

Chrome Cache Entry: 157

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 17 x 25, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	471
Entropy (8bit):	7.197252382638843
Encrypted:	false
SSDEEP:	12:6v/7eM/H/HTOlHAbsnwpncDR1pxInjqrrgRRIEw6Jz:qHTO0Gwpnc7pOnjqngRR1nJz
MD5:	C651D60A08FF0F579E2EB9BE6043A3C6
SHA1:	E7BCBB896EEA20A4DC68EDD2EF5B336E92690A55
SHA-256:	7B4B6ADAA1DDA648143A18A52B51DFAAB54775BDB6284DFF5C869235CD385230
SHA-512:	017C29423F096A45AD5D1002B2F14E27A8298F144A962B78F46A96626A1027D5E4EC57468CD8F8C5B9E97461FA651452A1786CD9F5F76264652D03F55D516138
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....>.....sRGB.....gAMA.....a.....pHYs.....+.....tEXtSoftware.Adobe ImageReadyq.e<...GIDAT8O...@...;Wa.`.X....b..... A.F....K...a..t*{3.e...K .....C..0.....)~;.eYvP....L}.KAEQP.4..WYd....mV]..m....$M...`...C.$R.....`..dM.T....,RU..TU..`.'0.!...D[`p..W)D8,dv]Wt....\^v.$.s..`.i...!...D..e$.....$.8./..8....;..\6,...f|....n.....e. .M...g.O.9....q..&.....0.w...k...z....\.iZ..c.;.F...Uq7.'Y....X ....IEND.B`.

Chrome Cache Entry: 158

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1592
Entropy (8bit):	4.205005284721148
Encrypted:	false
SSDEEP:	48:ztSAS1OtmCtc7aIVmt4yyR9S2lKUyDWwh:RoOtmCtc7aCmVQHSRh
MD5:	4E48046CE74F4B89D45037C90576BFAC
SHA1:	4A41B3B51ED787F7B33294202DA72220C7CD2C32
SHA-256:	8E6DB1634F1812D42516778FC890010AA57F3E39914FB4803DF2C38ABBF56D93
SHA-512:	B2BBA2A68EDAA1A08CFA31ED058AFB5E6A3150AABB9A78DB9F5CCC2364186D44A015986A57707B57E2CC855FA7DA57861AD19FC4E7006C2C239C98063FE903CF
Malicious:	false

Reputation:	low
URL:	http://https://aadcdn.msftauth.net/shared/1.0/content/images/signin-options_3e3f6b73c3f310c31d2c4d131a8ab8c6.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="48" height="48" viewBox="0 0 48 48"><defs><style>.a{fill:none;}.b{fill:#404040;}</style></defs><rect class="a" wi dth="48" height="48"/><path class="b" d="M40,32.578V40H32V36H28V32H24V28.766A10.689,10.689,0,0,1,19,30a10.9,10.9,0,0,1-5.547-1.5,11.106,11.106,0,0,1-2.219-1.719A11.373,11.373,0,0,1,9.5,24.547a10.4,10.4,0,0,1-1.109-2.625A11.616,11.616,0,0,1,8,19a10.9,10.9,0,0,1,1.5-5.547,11.106,11.106,0,0,1,1.719-2.219A11.373, 11.373,0,0,1,13.453,9.5a10.4,10.4,0,0,1,2.625-1.109A11.616,11.616,0,0,1,19,8a10.9,10.9,0,0,1,5.547,1.5,11.106,11.106,0,0,1,2.219,1.719A11.373,11.373,0,0,1,28.5, 13.453a10.4,10.4,0,0,1,1.109,2.625A11.616,11.616,0,0,1,30,19a10.015,10.015,0,0,1-.125,1.578,10.879,10.879,0,0,1-.359,1.531Zm-2,.844L27.219,22.641a14.7 16,14.716,0,0,0,.562-1.782A7.751,7.751,0,0,0,28,19a8.786,8.786,0,0,0-.7-3.5,8.9,8.9,0,0,0-1.938-2.859A9.269,9.269,0,0,0,22.5,10.719,8.9,8.9,0,0,0,19,10a8.786,8. 786,0,0,0-3.5.7,8.9,8.9,0,0,0-2.859,1.938A9.269,9.269,0,0,0,0,0,

Chrome Cache Entry: 159

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	23063
Entropy (8bit):	4.7535440881548165
Encrypted:	false
SSDEEP:	384:GvUzYI+Vi4g1V5it1ONhA6w+Kv8i/4CYzLKL4DrLU0iTxZTAzIzrwDlTWMClQip9:bkON69kClQq8hDRJHp2tWU25Zt/gREVG
MD5:	90EA7274F19755002360945D54C2A0D7
SHA1:	647B5D8BF7D119A2C97895363A07A0C6EB8CD284
SHA-256:	40732E9DCFA704CF615E4691BB07AECFD1CC5E063220A46E4A7FF6560C77F5DB
SHA-512:	7474667800FF52A0031029CC338F81E1586F237EB07A49183008C8EC44A8F67B37E5E896573F089A50283DF96A1C8F185E53D667741331B647894532669E2C07
Malicious:	false
Reputation:	low
URL:	http://https://passwordreset.microsoftonline.com/WebResource.axd?d=PZp-UguzV3eilgC9jthUzRVid1Zp7Yrh6GnWr6UFT7HZeGKMaINHyYeiOoYl901XG1SgokATq5Nqn3NEpiSXniqMwkj7V_kjzBmM_w8PfSJW9srpOcEZZbp1FPwrN8XzdR0AFY0bHhANU64v3ZJk5Q2&t=638509456396079063
Preview:	function WebForm_PostBackOptions(eventTarget, eventArgument, validation, validationGroup, actionUrl, trackFocus, clientSubmit) {.. this.eventTarget = eventTarget;.. this.eventArgument = eventArgument;.. this.validation = validation;.. this.validationGroup = validationGroup;.. this.actionUrl = actionUrl;.. this.trackFocus = trackFocus;.. this.clientSubmit = clientSubmit;..}..function WebForm_DoPostBackWithOptions(options) {.. var validationResult = true;.. if (options.validation) {.. if (typeof(Page_ClientValidate) == 'function') {.. validationResult = Page_ClientValidate(options.validationGroup);.. }.. }.. if (validationResult) {.. if ((typeof(options.actionUrl) != "undefined") && (options.actionUrl != null) && (options.actionUrl.length > 0)) {.. theForm.action = options.actionUrl;.. }.. if (options.trackFocus) {.. var lastFocus = theForm.elements["__LASTFOCUS"];.. if ((typeo

Chrome Cache Entry: 160

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 352 x 3
Category:	dropped
Size (bytes):	3620
Entropy (8bit):	6.867828878374734
Encrypted:	false
SSDEEP:	48:ZumKaT5ezv47j2/ZiRDlq16x8XvEUcg777shHdpHVGJqFd:Eal647jPDlL8XvEUcg77kVGyd
MD5:	B540A8E518037192E32C4FE58BF2DBAB
SHA1:	3047C1DB97B86F6981E0AD2F96AF40CDF43511AF
SHA-256:	8737D721808655F37B333F08A90185699E7E8B9BDAAA15CDB63C8448B426F95D
SHA-512:	E3612D9E6809EC192F6E2D035290B730871C269A267115E4A5515CADB7E6E14E3DD4290A35ABAA8D14CF1FA3924DC76E11926AC341E0F6F372E9FC5434B546E5
Malicious:	false
Reputation:	low
Preview:	GIF89a`.....iii!.....!.&Edited with ezgif.com online GIF maker.!..NETSCAPE2.0.....,...`.....6.....P.I.....H....I..:qJ.....k....`BY..L*..&...!.....,...`.....9..i....Q4.....H..j.=.k9-5_.. .....j7..({.....!.....,...`.....9.....trV.....H....`.[.q6.....>.. .CZ.&!.....M...!.....,...`.....8.....:.....H..jJ..U..6_...../.el...q.)...*..!.....,...`.....9....i..l.go.....H..*".U...f....._.....5 .....n..!.....,...`.....:..i...../.....H...5%.kE/5.....In.a..@&3.....J...!.....,...`.....9.....kr.j.....H..*.-.{Im5c.....@&.....!.....,...`.....9.....j..q....H...].&..\.5.....8..S.....!. .....,...`.....9.....3q.g..5....H...:u.....Al..x.q.....!.....,...`.....9.....\.F....z....H...zX...ov.....h3N.x4.....j..!.....,...`.....9.....Q.:.....H....y..^...1.....n.!.F.....E...!.....,.. ..`.....8.....i,.....H....*_.21.I.....%...

Chrome Cache Entry: 161

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 89 x 18, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1805
Entropy (8bit):	7.265265285391204
Encrypted:	false
SSDEEP:	24:oV1hpunQWwjx82lY2T32HEV8KJyJ3VAyKOGpxbAKJcyIXRP6VEBxX4pAE60KKAU9:4itNn2VMJ3R6breHDBBThFtYeD5B2
MD5:	BC89C1FBFBC227DC5A7ED9B2797E240D

SHA1:	8A9390297FDD0963C466CF2FD35D5B1F88A46B6A
SHA-256:	744A8CD0A4D15DFCF4A5D2E832FF556D950F8AF24D7B66104AB2EF4FE2605D9A
SHA-512:	C18F6B22F4AC5040E3FEBE8034AD3A3A3EF32CF3384BE6C3144B2EB04080F03111743D5B30AF3A1343AFD68A20AAE5972422C724107243D00CD9CF263DDC100 7
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...Y.....0.r.....sRGB.....gAMA.....a.....tEXtSoftware.Adobe ImageReadyq.e<... iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpC ehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.0-c060 61.134777, 2010/02/12-17:32:00 "> <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/m m/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CS5 Windows" xmpMM:InstanceID="xmp.iid:BABFACAF90151 1E2BD4FDE5C526470CF" xmpMM:DocumentID="xmp.did:BABFACB0901511E2BD4FDE5C526470CF"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:BAB FACAD901511E2BD4FDE5C526470CF" stRef:documentID="xmp.did:BABFACAE901511E2BD4FDE5C526470CF"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xp acket end="r"?>..R....fIDATXG.mq[1.E.!...3&...P.....3..~L..q.O..t..{...v?..n.....b#.-.i..

Chrome Cache Entry: 162

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	379
Entropy (8bit):	4.942805876241154
Encrypted:	false
SSDEEP:	6:tI9mc4slztdbC/yXADQKDTcVEq0FyX4bVGEynbtwag8R+mkbtR1dI1zAmiadc:t4pb8WsQKvkB0wX4gEkbtLv8mkbtvdIe
MD5:	2D8F86059BE176833897099EE6DDEDEB
SHA1:	93A2E327027DEED53076E86BFA7D9EEBBF0CC4B9
SHA-256:	34D8DA073F47030EE94B99D84FBE68E3345BD8AAA37EA909FF2DA00238447486
SHA-512:	64D75B1F35180FF61F5BF11D21544454DF016D0854573D75D277FCB933CE845D1436BDC822445B78C627A1FF730B39FC34B72C27D45A39E237F2CCF0876FCA4E
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msftauth.net/shared/1.0/content/images/picker_account_msa_3b879963b4f70829fd7a25cbc9519792.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="48" height="48" viewBox="0 0 48 48"><title>assets</title><circle cx="24" cy="24" r="24" fill="#e6e6e6"/><path d=" M13.44,36h1.92a8.64,8.64,0,0,1,1,17.28,0h1.92a10.573,10.573,0,0,0-6.569-9.771,7.68,7.68,0,1,0-7.982,0A10.573,10.573,0,0,0,13.44,36Zm4.8-16.32A5.76,5.76,0,0,1,1,24,2 5.44,5.766,5.766,0,0,1,18.24,19.68Z" fill="#404040"/></svg>

Chrome Cache Entry: 163

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (2054)
Category:	downloaded
Size (bytes):	9285
Entropy (8bit):	5.397876465825329
Encrypted:	false
SSDEEP:	192:U23y7LVYADenIY9uOqc4gIVH4VoXLIOjMuj4IMNVWmn4GHF5y8WC:U23y7hDTYvquI14i5EOvWmNl5y8h
MD5:	439A53994F1A9C860C7787ED5100CA0C
SHA1:	15BA120F64BBF6A59A457841B10DF0D6D1B4574C
SHA-256:	441BFA485FB0EB8AD2BE7001209868B57C41769CAE9512A774419F5882C093E6
SHA-512:	FB6002797BD9E28A352BCBE4643BC7E998C562218D9189AE879E1DC605BC79C3234435029B46667724E5C85A475A72C8DDDED17E3EEFD7791EC1FB21822D38 4
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/watson.min_q5ptmu8aniymd4ftuqdkda2.js
Preview:	!function(){function e(){return(x.location.protocol||"").concat("//",x.location.hostname||x.location.host)}function r(e){if(e){try{var r=/function (.{1,})\(/,n=r.exec(e.constructor .toString());return n&&n.length>1?n[1]:""}catch(e){}}return""}function n(e,r,n){if(e&&r){n||(e=e.toLowerCase());for(var t=0;t<r.length;t++){var o=r[t];if(o&&(n||(o=o.toLo werCase()),e.indexOf(o)>=0)){return r[t]}}}return null}function t(e,r,n){return!!(0===n&&r&&r.indexOf("Script error.")>=0)}function o(e,r){.if(!e.expectedVersion||e.expec tedVersion!==E().jquery){if(r&&r.indexOf("jQuery.easing[jQuery.easing.def] is not a function")>=0){return!0}if(r&&r.indexOf("The bound jQuery version is not the expected version -- loaded")>=0){return!0}}return!1}function i(e){if(e){try{if("string"!==E.type(e)&&JSON&&JSON.stringify){var n=r(e),t=JSON.stringify(e);return t&&"{}"!==t||(e.error&& (e=e.error,n=r(e)),(t=JSON.stringify(e))&&"{}"!==t||(t=e.toString())),n+":"+t}}catch(e){}}return""+(e||"")}function a(e,r){return{."sig

Chrome Cache Entry: 164

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (43896)
Category:	downloaded
Size (bytes):	223759
Entropy (8bit):	5.257015244909601
Encrypted:	false

SSDEEP:	3072:5Q0ZqoBmLJEoWcjY6B66pO25rksurxIDZVihYZ+V:RmNdTpOFsursZkV
MD5:	764E526CEF65C9F062BB8E83D8EBCE0B
SHA1:	F5166F7B003CBE1B171BE88AA65D2E3FD2331366
SHA-256:	474CE0790CEB18A100CEBAF1AC0915A51389FCAE0830C3B44BFA1E365D40B2B4
SHA-512:	49725A491D8C7494D4074D0A96D978D75700657CA9EDA456C3B3EBA3333DC6733D19A8BBE19BC9DCF381FA1B1CA96251A910056ADE259340A17F85FB6D5EF83
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msftauth.net/shared/1.0/content/js/asyncchunk/convergedlogin_pcustomizationloader_8e14dcf0e3ff5580d170.js
Preview:	/*!. * ---------- START OF THIRD PARTY NOTICE ----------. * . * This file is based on or incorporates material from the project listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise.. * . * json2.js (2016-05-01). * https://github.com/douglascrockford/JSON-js. * License: Public Domain. * . * Provided for Informational Purposes Only. * . * ---------- END OF THIRD PARTY NOTICE ----------. */.(window.webpackJsonp=window.webpackJsonp||[]).push([[8],{529:function(e,t,r)

Chrome Cache Entry: 165

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65450), with CRLF line terminators
Category:	downloaded
Size (bytes):	119648
Entropy (8bit):	5.356165204896218
Encrypted:	false
SSDEEP:	3072:/Yh8eip3huuf6lidlrvakdtQ47GKvPhQDvMwFdm:/i8eGRuufsr5zQ47GKvPyDvG
MD5:	75CF78D0E38C65A538AD253CA9E48DBE
SHA1:	BF0452E4A42A9AF3B69D5D8C3A3A0433F14921B6
SHA-256:	DF2AA8537C1992C94846A0FFFFAA9031D430D9D0210B9E396EC059AFF62627E0
SHA-512:	81383E4FDAE1F34F8E652F69058D57A2A4BD0A77C2C41C3174BEE0CEBA83A8326229C2A74EAF415BFBD34382B1C442A97C41034F43CD77A391BA9B4DAAE65463
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/watsonsupportwithjquery.3.5.min_dc940oomzau4rsu8qesnvg2.js
Preview:	/*! jQuery v3.5.1 | (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(C,e){"use strict";var t=[],r=Object.getPrototypeOf,s=t.slice,g=t.flat?function(e){return t.flat.call(e)}:function(e){return t.concat.apply([],e)},u=t.push,i=t.indexOf,n={},o=n.toString,v=n.hasOwnProperty,a=v.toString,l=a.call(Object),y={},m=function(e){return"function"==typeof e&&"number"!=typeof e.nodeType},x=function(e){return null!=e&&e===e.window},E=C.document,c={type:!0,src:!0,nonce:!0,noModule:!0};function b(e,t,n){var r,i,o=(n=n||E).createElement("script");if(o.text=e,t)for(r in c)(i=t[r]||t.getAttribute&&t.getAttribute(r))&&o.setAttribute(r,i);n.head.appendChild(o).parentNode.removeChild(o)}function w(e){return null==e?e+"":"

Chrome Cache Entry: 166

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	3005
Entropy (8bit):	4.3348196756520005
Encrypted:	false
SSDEEP:	48:ITWNX9q7aVxyFGwvqNTTswh11KdA/IMUitKhyWirt+NG/BC0/PTfhyr1+18:liNX9oFG4qTJb0a/IMNURkt6GJZ/7fU7
MD5:	A870B45AC5D6B0D4E18C4829C7B660B4
SHA1:	2D3CA0E1F19EFDEB9B2DD3DCFFB17F8ABA118AA0
SHA-256:	144524233F795D6A425B76F7AE5C0BB622B5F67E2E6AE73532AD526528CA07CF
SHA-512:	295A21307D452F4BF51C62770C6A6B43CDB8B5A6BFA3617E068C8550285252B88F8BBF93A81C39E4BD7F73645EE094EDE0E2733DAFA5094E3EBAE2003336327
Malicious:	false
Reputation:	low
URL:	http://https://passwordreset.microsoftonline.com/WebResource.axd?d=YNhUFlNXinz8LgHwbL24RQH-ZbXxyvcr7OOnguhxng8ZuiFTPNJ9QXh8dtoptfX3BeFWG9A9Hk63eLbtblxk0HvJhkP2FoYJavizwe94hutTawufYPfHJsHAawGlkTxEe6yX2kZBiYdQxl60gLHN2g2&t=638509456396079063
Preview:	function WebForm_FindFirstFocusableChild(control) {.. if (!control || !(control.tagName)) {.. return null;.. }.. var tagName = control.tagName.toLowerCase();.. if (tagName == "undefined") {.. return null;.. }.. var children = control.childNodes;.. if (children) {.. for (var i = 0; i < children.length; i++) {.. try {.. if (WebForm_CanFocus(children[i])) {.. return children[i];.. }.. else {.. var focused = WebForm_FindFirstFocusableChild(children[i]);.. if (WebForm_CanFocus(focused)) {.. return focused;.. }.. }.. } catch (e) {.. }.. }.. }.. return null;..}..function WebForm_AutoFocus(focusId) {.. var targetControl;.. if (__nonMSDOMBrowser) {.. targetControl = document.getElementById(focusId);.. }.. else {.. targetContro

Chrome Cache Entry: 167

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

File Type:	MS Windows icon resource - 6 icons, -128x-128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsQZp:nfgyyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD(1
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msftauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico
Preview:	.....h(..f...HH.....(..00.....h....6.. .....=.....@.....(....A..(.....(......"P.....""" ...3 3333333333333333333333333333333""" ...3333333333333333333333333333333""" ...3333333333333333333333333333333""""" """ ...3333333333333333333333333333333""" ...3333333333333333333333333333333""" ...33333333333 3333333333333333333""" ...3333333333333333333333333333333""" ...3333333333333333333333333333333""""""""""""""" """ ...3333333333333333333333333333333""" ...3333333333333333333333333333333""" ...33333333333 3333333333333333333""" ...3333333333333333333333333333333""

Chrome Cache Entry: 168	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 89 x 18, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1805
Entropy (8bit):	7.265265285391204
Encrypted:	false
SSDEEP:	24:oV1hpunQWwjx82lY2T32HEV8KJyJ3VAyKOGpxbAKJcyIXRP6VEBxX4pAE60KKAU9:4itNn2VMJ3R6breHDBBThFtYeD5B2
MD5:	BC89C1FBFBC227DC5A7ED9B2797E240D
SHA1:	8A9390297FDD0963C466CF2FD35D5B1F88A46B6A
SHA-256:	744A8CD0A4D15DFCF4A5D2E832FF556D950F8AF24D7B66104AB2EF4FE2605D9A
SHA-512:	C18F6B22F4AC5040E3FEBE8034AD3A3A3EF32CF3384BE6C3144B2EB04080F03111743D5B30AF3A1343AFD68A20AAE5972422C724107243D00CD9CF263DDC10(7
Malicious:	false
Reputation:	low
URL:	http://https://passwordreset.microsoftonline.com/images/header_Microsoft.png
Preview:	.PNG.....IHDR...Y.....0.r.....sRGB.....gAMA.....a.....tEXtSoftware.Adobe ImageReadyq.e<... iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpC ehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.0-c060 61.134777, 2010/02/12-17:32:00 "> <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/m m/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CS5 Windows" xmpMM:InstanceID="xmp.iid:BABFACAF90151 1E2BD4FDE5C526470CF" xmpMM:DocumentID="xmp.did:BABFACB0901511E2BD4FDE5C526470CF"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:BAB FACAD901511E2BD4FDE5C526470CF" stRef:documentID="xmp.did:BABFACAE901511E2BD4FDE5C526470CF"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xp acket end="r"?>..R....fIDATXG.mq[1.E.!...3&...P.....3..~L..q.O..t..{...v?..n.....b#.-.i..

Chrome Cache Entry: 169	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, Unicode text, UTF-8 text, with very long lines (1094), with CRLF line terminators
Category:	downloaded
Size (bytes):	52293
Entropy (8bit):	4.6946447418827715
Encrypted:	false
SSDEEP:	768:3VNB5cxEwIRvL5IBRe7RMCb9ElQfWGfAlBRsYXzrSSl:3VAErRCBRe7eCelQfWGfAlBRsYX6Sl
MD5:	FE85DF425B95297E7D7E388A7C0D6DE5
SHA1:	3C9680147BBEA42B2E764A995119D89188F01A6C
SHA-256:	352B8A2025EDDD7FCF2883FAC22EF9A0AEB5C3A38F238E016EACD9BA1B582214
SHA-512:	D580F7437D0A379448BDB907C4D5EC9522335C9012E4069F94A13FD5A997B2CD9FAAE552E7D122D1087B318CFFFD0C1386977C8B089401A727C6769E8D920D4
Malicious:	false
Reputation:	low

URL:	http://https://passwordreset.microsoftonline.com/?ru=https%3a%2f%2flogin.microsoftonline.com%2ffd4efb89-68eb-42bb-bd22-018f0e50365b%2freprocess%3fctx%3drQQIARAAnVE_aNRgHE2aa-ydrT3q4ljOTj1z-ZJ8Sb4cdMi_04ras3-gnsiRP1_aeJdLmqTtXUsXdRAE6eyidnDoJlJYqqJzcegm3CxSO4h06qZ3uDgW3w8ej9_weLw3SXElrjwB_kJg-swAz-MYB_fVP4jHcvmXxW-X31aJ6k73Q-tr5cnDXVJZTtMoKbPs_cBa92PcxEnCBJ1SsmzFOAr9VlpywoCte2EcJKyLPWu1mZasJGrvkeQhSR6R5O7AiimpvCbysqYJECq6yvOaaZgQlE6ReEM3ZQlVOGTK0ORltfdjZEkSdQNAiHQJGBJSDFip6DpSRUNRFQVJOqfpmtQ7uWeHKrpqQN2AUNAMTRVNvjswOqOupst8n8LY38AnA9l-xnoUJukzKjNjgPVd6kzFvKEmPBdiz0YKlyFsM5C3bcZ2eZ4BHPIAFoEgifYBRYcRbvnuYYY8zgwDqjw0lMsTl4hx4jRD7gz26qW-f9z7RL9Tn_64-GX8_XXiYJBV51bWOq1bSzP29Ea7eGceuKo8JwZsI8Li_A2cWI0FVujUlAUOTEllbpsmt2l6n84OUXmiQOlV7hdNPj5H7Gf_f6jD82R3mMtlndCOrZbru2MTHGe7CCCBQTIGDORskbFtGTHAdqDgIAthZHWHYY52mpYfJGOTmwXfradhA7cK5c1CO0jqjtNXa1ZzFSeF8t1CL2rh3tbW1oORM7l_HiFOLxy9eHXy-9Hzn9eOR6_UrGrnqrbeuA2XikUnmk1qi8XZxZuNtoDnKpEcgXRaEWqRHBfVqdd54g81&mkt=en-US&hosted=0&device_platform=Windows+10
Preview:	..<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">..<html xmlns="http://www.w3.org/1999/xhtml" dir="ltr" lang="en-US">..<head><title>...Microsoft Online Password Reset..</title><meta http-equiv="x-ua-compatible" content="IE=9" /><meta http-equiv="Expires" content="0" /><meta http-equiv="Pragma" content="no-cache" /><meta http-equiv="Cache-Control" content="no-store, no-cache" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta name="robots" content="noindex, nofollow, NOODP, NOYDIR" /><meta name="viewport" content="width=device-width, initial-scale=1" /><link id="FavoriteIcon" rel="Shortcut Icon" type="image/x-icon" href="favicon.ico?v=1342177280" />.... <script src="//ajax.aspnetcdn.com/ajax/jQuery/jquery-3.6.0.min.js" type="text/javascript"></script>.. <script type="text/javascript">window.jQuery || document.write('<script type="text/javascript" src="js/jquery-3.6.0.min.js">\x3C/sc

Chrome Cache Entry: 170

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12429
Entropy (8bit):	4.880328887313854
Encrypted:	false
SSDEEP:	192:x8GsutherY4/qX0Ii8tPNS3ndq3yFwmLkwjPuqwnESBX3Sri6K4Cl44B6QRguaZ:xBjiUSCDnyQRq
MD5:	A17520454D4A65A399B863B5CC46D3FC
SHA1:	0A02C72D7AFCD5198C590108E7F2302A1F75544D
SHA-256:	62E5E7DC19D018BEDB24E2C89ED41271B9D94A6DDE3359CC9CABBC315385C0E5
SHA-512:	0757698DC40D0AC165F159270375514A543448FB2A3E7B3B70EB500180EA00FDA3A4FC7F77C48EA013C3BAC082C092BB852CF86F7D4C0094596DE6917DCA144
Malicious:	false
Reputation:	low
URL:	http://https://passwordreset.microsoftonline.com/css/Style.css?v=1342177280
Preview:	* {.. line-break: strict..}....body,..input,..select,..textarea,..button,..legend {.. font-weight: normal;.. font-family: "Segoe UI-Regular-final", "Segoe UI", Segoe, Tahoma, Helvetica, Arial, Sans-Serif;.. font-size: 12px;.. line-height: 19px;.. letter-spacing: .01em;.. color: #666666..}....span.requiredstar {.. font-weight: normal;.. font-family: "Segoe UI-Regular-final", "Segoe UI", Segoe, Tahoma, Helvetica, Arial, Sans-Serif;.. font-size: 12px;.. color: #a80f22..}....h1,..h2,..h3,..h4,..h5,..h6 {.. font-weight: normal;.. font-family: "SegoeUI-Light-final", "Segoe UI Light", "Segoe UI", Segoe, Tahoma, Helvetica, Arial, Sans-Serif;.. color: #333333;.. margin: 0 0 0 0;.. cursor: default..}....h1 {.. font-size: 32px;.. line-height: normal;.. letter-spacing: -.01em;.. padding-left: 0px;.. padding-right: 0px..}....h2 {.. font-size: 22px;.. line-height: normal;.. letter-spacing: -.01em..}....h3 {.. font-size: 13px;

Chrome Cache Entry: 171

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 444890
Category:	downloaded
Size (bytes):	121438
Entropy (8bit):	**7.997495520894356**
Encrypted:	**true**
SSDEEP:	3072:yb/jE8LbFLCp5Lognxe6+YoD1tJj/hLK1V:crFCTLo2Jg1tJj/9K1V
MD5:	9D04112039AA1DB4EA5F49C521125D6A
SHA1:	D3BBFB157E00A0BA12A53AEE8BC05711849B51F0
SHA-256:	DFB209628564E6F287D8154B1DD0CAEA878E9FEB3EA65BDF16E49EC4354CEF69
SHA-512:	AE3C580DF190EB8EA393E669195F845FAD5A19350DCBE9FF5332BE019243CC0057A2567109A01E1BA9CC77E6F393F632A4DE6531F237F1DE08480CABCA60DF45
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msauth.net/shared/1.0/content/js/ConvergedLogin_PCore_T2EBBtMmyv072RjbQwNpoQ2.js
Preview:	.....m[.H....~...1v#\..-Z...Ul.f0t.....R..%.$.2.../"2SJ.2U5.w..s.;.....Si...+.n..7..i.....q.....t9.9..\|.=.(....K..g%.;.c...F%/p.h.Fv.....<./M.pVJ.Yi...2'.K..'Ph...T..".teG.[..R.....M..J;...~?&. L<.....\|..bVZ...J/...X..(..IR...gh$^@z...dG....4.....Z.!..5.fx.1.C.=.*..@._...b....4.....t".....C).Ko.B.>...LK..YL.`zV.t.]8I57.E..E./.....Y1...^....o.id..r..L.=.... ..y....J.I.....%.'.|.|.[...YU.A..g....q.\....Zk.fTx.c..c....<..U'.}r...c....s?..hx..g...s\.....zP:.g....T...%.?..K..X..>N......"p.ceVY.....W...m@.....zl.t..?....>....A..W.....c\5U..$L...h...P2g@LU..l.^ew...ww..\|.?...Z.....`.. .RT..*#=.*.....".B5.....=.8...$.J.....+....Y[..h.....%.((..*.),...J[.d-=3.}s..E..\..D!.....,'.z.;...o.....2.....G...d...-%,u.a4...v,..'..*.c..-`/..H=."@.....>.A;A~.Do..B`K.q...Sq5....!*..1..t..8...>.....ZK;\.i..O.OY...h.j...[9....Db.....L.>..M...t.0%+.$.Ta.3+z..!.B=ZUt7t...Gf.V...=.....'.....K{....i.\o..S.dH....].,

Chrome Cache Entry: 172

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 338 x 72, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4020

Entropy (8bit):	7.929907559552797
Encrypted:	false
SSDEEP:	96:1X+Yg6let+ZpBmQKEuhA/4oJqNoCkQV+CX8h:Fg69t+YfPhEBPnC+t
MD5:	36AFB641BECFAD75FED5F4E6E8C39268
SHA1:	2495652F017B7A06D796AFE9C4A06ECD54F9CCFE
SHA-256:	5C2192A3932CB78B431A1AC0F3F3D73414A31C63D5CB279F2687E58C72694200
SHA-512:	08C27020CF80A181B941EE144090FFBDD12ED34BA8CBEC037ACECE63F850FF8A69BE6DDB0EC24F7141C46F27779ED59AF84A55FB367C1B6F8893B444F44C5A F5
Malicious:	false
Reputation:	low
URL:	http://https://passwordreset.microsoftonline.com/images/footer_logo_grey_bg.png
Preview:	.PNG.....IHDR...R...H.....}.....pHYs..!8..!8.E.1`....sRGB.....gAMA.....a....IIDATx...r....[ZZ..V.'0.....].....z....M..U.%.....C.....}...s...mIV.O5..... ...U.Hq@b.....Y..../)..hy.._S.....KzK...O\5EQ...(....B.(.....(J *...(...*....B.(.....(J *...(...*....B.(..H..EQ.C...V...7.//...~...?.....h4:.@TH.E....}.....k.v....L./.@TH...pGN.;....'.(s...k.....4GTH...'O.~...g[..o..''....I..>.G...;..~...&.....d..u.^F.....M.h.....>.}>.....[.....E.b..?.u..{.B.....M._.iAh.>~.<*S...=.@`e..e....R....._ViA.E....R.@...@..vm.'Ei.v..\>QD..e..R.....;o.p{...../^d..TH;., F>..6...1?..E.p.}..J.p...XD.....7*.^b..../.w.....n0.+R.V).J.a..^.X.S..B(..W+++..W. ..e%"Z.[.{,....JQ.iG`....(5..e..`u.*.=.)J.....C.!.@..;$.i.F...W.[....#.....k.(J.z....`.dB..)..- H...R.H..O.#V..%.....W.4>.'..aJ9.2Q..+.R..id`.x..1.. .../.(J%..>2d.QJ..7.|.S`..10>..}.M#.....4.....<f}..OWO..m.;C[;u.|P!.....L...S.Egr.....3.k.....i.....O...

Chrome Cache Entry: 173

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 352 x 3
Category:	downloaded
Size (bytes):	2672
Entropy (8bit):	6.640973516071413
Encrypted:	false
SSDEEP:	48:ZaOdwduTYPpS9pZy9vDNi1miicsvrJkafMiS+MGQ09DU/X9/4Xp6m5Z9SQcq:4CIuTYPpSTc9vcPZX9/2gzQ/
MD5:	166DE53471265253AB3A456DEFE6DA23
SHA1:	17C6DF4D7CCF1FA2C9EFD716FBAE0FC2C71C8D6D
SHA-256:	A46201581A7C7C667FD42787CD1E9ADF2F6BF809EFB7596E61A03E8DBA9ADA13
SHA-512:	80978C1D262BC225A8BA1758DF546E27B5BE8D84CBCF7E6044910E5E05E04AFFEFEC3C0DA0818145EB8A917E1A8D90F4BAC833B64A1F6DE97AD3D5FC80A02 308
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msftauth.net/shared/1.0/content/images/marching_ants_white_8257b0707cbe1d0bd2661b80068676fe.gif
Preview:	GIF89a`.....!..NETSCAPE2.0.....!.....,....`.....6.....P.I.....H....I..:qJ.....k....`BY..L*..&...!.....,....0.....<....[.\K8j.tr.g..!.....,....3.....^;.*..\UK.]\.%.V.c...!.....,....7..... ...`....lo...[.a..*Rw~i...!.....,....;.....h.....I.G-.[K.,_XA]..'g..!.....,....?.....i.....g....Z.}..)..u...F..!.....,....C.....P..nt^.i....Xq...i..!.....,....F.....{^b....n.y..i...\C.-...!.....,... .H.....R...o....h.xV!.z#...!.....,"...L.....r.jY..w~aP(.....[i...!.....,(...N.....r....w.aP.j.').Y..S..!.....,....H.....`.....hew..9`.%z.xVeS..!.....,5...A.....`...\m .Vmtzw.}.d.%...Q..!.....,9...=.....h.....3S..s.-W8m...Q..!.....,A...5.....h.....N...:..!..U..!.....,H.....h....M.x...f.i.4..!.....,O...'.....i...tp.....(..!.....,X.....j...@.x....! .....,]....j..L..3em..!.....,e.....`.....!.....,n.....{i..!..

Chrome Cache Entry: 174

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (3757)
Category:	downloaded
Size (bytes):	4730
Entropy (8bit):	5.122007329309551
Encrypted:	false
SSDEEP:	96:jPjDXOMS1WfyPlZ6fWRW8a1RwCEL3Aa1Rj1LjpVSzC:jP7slZPA2LtjLNVSzC
MD5:	3631AA6B55B811946DE4FC289031778B
SHA1:	8CD792280A0594585289DBA2748D51FE81904AC7
SHA-256:	3957106AD7B920D6D8E73EF7B9DE532CAE05E78DF5DB847777F73193AA4086A8
SHA-512:	A67060060D97C0F1AC9B99592AEB23886CEA70962EFEC3DD7C793E91EEB3F965D495D2741BA6EB003E4E6243C2A6CF857491332E14C2822A9FA3D6BF2747FD3 E
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msftauth.net/shared/1.0/content/js/asyncchunk/convergedlogin_presetpasswordsplitter_f7fbb7540d7be2ae771b.js
Preview:	/*!. * --- START OF THIRD PARTY NOTICE --. * . * This file is based on or incorporates material from the project listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise.. * . * json2.js (2016-05-01). * https://github.com/douglascrockfor d/JSON-js. * License: Public Domain. * . * Provided for Informational Purposes Only. * . * --- END OF THIRD PARTY NOTICE ---------- ----------. */.(window.webpackJsonp=window.webpackJsonp||[]).push([[36],{499:function(t,e,i

Chrome Cache Entry: 175

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

File Type:	PNG image data, 17 x 25, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	471
Entropy (8bit):	7.197252382638843
Encrypted:	false
SSDEEP:	12:6v/7eM/H/HTOlHAbsnwpncDR1pxInjqrrgRRIEw6Jz:qHTO0Gwpnc7pOnjqngRR1nJz
MD5:	C651D60A08FF0F579E2EB9BE6043A3C6
SHA1:	E7BCBB896EEA20A4DC68EDD2EF5B336E92690A55
SHA-256:	7B4B6ADAA1DDA648143A18A52B51DFAAB54775BDB6284DFF5C869235CD385230
SHA-512:	017C29423F096A45AD5D1002B2F14E27A8298F144A962B78F46A96626A1027D5E4EC57468CD8F8C5B9E97461FA651452A1786CD9F5F76264652D03F55D516138
Malicious:	false
Reputation:	low
URL:	http://https://passwordreset.microsoftonline.com/images/hip_reload.png
Preview:	.PNG.....IHDR.....>.....sRGB.....gAMA.....a.....pHYs.....+.....tEXtSoftware.Adobe ImageReadyq.e<...GIDAT8O...@...;Wa.`.X....b..... A.F....K...a..t*{3.e...K .....C..0.....)~;.eYvP....L}.KAEQP.4..WYd....mV]..m....$M...`...C.$R.....`..dM.T....,RU..TU..`.'0.!...D[`p..W)D8,dv]Wt....\^v.$.s..`.i...!...D..e$.....$.8../..8....;..\6,...f\....n.....e. .M...g.O.9....q..&.....0.w...k...z....\.iZ..c.;.F...Uq7.'Y....X ....IEND.B`.

Chrome Cache Entry: 176

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1592
Entropy (8bit):	4.205005284721148
Encrypted:	false
SSDEEP:	48:ztSAS1OtmCtc7aIVmt4yyR9S2lKUyDWwh:RoOtmCtc7aCmVQHSRh
MD5:	4E48046CE74F4B89D45037C90576BFAC
SHA1:	4A41B3B51ED787F7B33294202DA72220C7CD2C32
SHA-256:	8E6DB1634F1812D42516778FC890010AA57F3E39914FB4803DF2C38ABBF56D93
SHA-512:	B2BBA2A68EDAA1A08CFA31ED058AFB5E6A3150AABB9A78DB9F5CCC2364186D44A015986A57707B57E2CC855FA7DA57861AD19FC4E7006C2C239C98063FE903CF
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="48" height="48" viewBox="0 0 48 48"><defs><style>.a{fill:none;}.b{fill:#404040;}</style></defs><rect class="a" width="48" height="48"/><path class="b" d="M40,32.578V40H32V36H28V32H24V28.766A10.689,10.689,0,0,1,19,30a10.9,10.9,0,0,1-5.547-1.5,11.106,11.106,0,0,1-2.219-1.719A11.373,11.373,0,0,1,9.5,24.547a10.4,10.4,0,0,1-1.109-2.625A11.616,11.616,0,0,1,8,19a10.9,10.9,0,0,1,1.5-5.547,11.106,11.106,0,0,1,1.719-2.219A11.373,11.373,0,0,1,13.453,9.5a10.4,10.4,0,0,1,2.625-1.109A11.616,11.616,0,0,1,19,8a10.9,10.9,0,0,1,5.547,1.5,11.106,11.106,0,0,1,2.219,1.719A11.373,11.373,0,0,1,28.5,13.453a10.4,10.4,0,0,1,1.109,2.625A11.616,11.616,0,0,1,30,19a10.015,10.015,0,0,1-.125,1.578,10.879,10.879,0,0,1-.359,1.531Zm-2,.844L27.219,22.641a14.716,14.716,0,0,0,.562-1.782A7.751,7.751,0,0,0,28,19a8.786,8.786,0,0,0-.7-3.5,8.9,8.9,0,0,0-1.938-2.859A9.269,9.269,0,0,0,22.5,10.719,8.9,8.9,0,0,0,19,10a8.786,8.786,0,0,0-3.5.7,8.9,8.9,0,0,0-2.859,1.938A9.269,9.269,0,0,0,0,19Z" transform="translate(0 0)"/></svg>

Chrome Cache Entry: 177

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (14735)
Category:	downloaded
Size (bytes):	15708
Entropy (8bit):	5.367272167361047
Encrypted:	false
SSDEEP:	384:DDeX/4OSgcw2Z12CvfeXOh+rF3lsdDZDFzfXdv79dC:2/gFb57PC
MD5:	5316E62A0EED2307FB8BCD111E96CB8F
SHA1:	71240D69183FDCCB39FE26A96045734C431A3F56
SHA-256:	35AFB11DAB6EDCBC989A25FE5CF19F5D8289499232B7EC775F318D8B8A5BBF78
SHA-512:	0AA96D93A32DB7D0F73FFF77C9EDD2B4ACC315532B2472B26601FC669088062AEA15F3AF62CB407165254D1B251BFA94790667D4CDDD5000C624F1138ADD55
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msftauth.net/shared/1.0/content/js/asyncchunk/convergedlogin_pfetchsessionsprogress_7c1aa7609345f99e4914.js
Preview:	/*!. * --- START OF THIRD PARTY NOTICE ---. * . * This file is based on or incorporates material from the project listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise.. * . * json2.js (2016-05-01). * https://github.com/douglascrockford/JSON-js. * License: Public Domain. * . * Provided for Informational Purposes Only. * . * --- END OF THIRD PARTY NOTICE ---. */.(window.webpackJsonp=window.webpackJsonp||[]).push([[17],{515:function(e,n,s

Chrome Cache Entry: 178

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 16 x 25, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	405
Entropy (8bit):	6.927238031773719
Encrypted:	false
SSDEEP:	6:6v/lhPGtyR8R/Chm+jnDs9cCXz6fXIpvI+WOcy0f11VTaENo+7PfW3e37zt1afwp:6v/7SyG/HYfXJOvU1zTa8o+W8
MD5:	D4FFE61373F6AA32EEB8CA7CD41AB980
SHA1:	4925FAC4BC73EFB7C7BBC32B11C435ECF1D61674
SHA-256:	D5C54FFC6B8BD44D932BE8F37B1CD5B666205C7574F9D56EF68E56F83E08FFAD
SHA-512:	0F7EDE96F20BB3C053C246FFE1EF8CE739CEF7757FAAED031A365299B88664A046557C2C7FDB3BADED070BA4EBA1A14950D7E3A066B4976BF07142CEFA48BEEB
Malicious:	false
Reputation:	low
URL:	http://https://passwordreset.microsoftonline.com/images/hip_speaker.png
Preview:	.PNG.....IHDR.....8.....sRGB.....gAMA.....a.....pHYs.....+.....tEXtSoftware.Adobe ImageReadyq.e<....IDAT8O...0...nf..y.,X4.g.l.h4..H.`.b.bA..f.n....%.=.iS.?N....^....A.(...~.i..m[.Qyz..iB..(...8...<G.....y..$.8....EQ.u]..I..(R.I...a...=..?t...CUU.....-..7.!..@.u0\..y.@..[a...p@.J.....e..>.Y..i..>A...+.,[. X9..z....B.4..+)..`n/..Q..>...y....e<....IEND.B`.

Chrome Cache Entry: 179

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	36
Entropy (8bit):	4.503258334775644
Encrypted:	false
SSDEEP:	3:Eq62iczBr9ks:EqdiczBys
MD5:	06B313E93DD76909460FBFC0CD98CB6B
SHA1:	C4F9B2BBD840A4328F85F54873C434336A193888
SHA-256:	B4532478707B495D0BB1C21C314AEF959DD1A5E0F66E52DAD5FC332C8B697CBA
SHA-512:	EFD7E8195D9C126883C71FED3EFEDE55916848B784F8434ED2677DF5004436F7EDE9F80277CB4675C4DEB8F243B2705A3806B412FAA8842E039E9DC467C1164
Malicious:	false
Reputation:	low
URL:	http://https://content-autofill.googleapis.com/v1/pages/ChVDaHJvbWUvMTE3LjAuNTkzOC4xMzISFwmCAmly1gHbXRIFDdFbUVISBQ1Xevf9?alt=proto
Preview:	ChgKDQ3RW1FSGgQIVhgCIAEKBw1Xevf9GgA=

Chrome Cache Entry: 180

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 4 icons, 64x64, 32 bits/pixel, 32x32, 32 bits/pixel
Category:	dropped
Size (bytes):	24038
Entropy (8bit):	5.992474931914016
Encrypted:	false
SSDEEP:	384:cLU4fKWVUvyZk56/1+fZfMj8hTb5nz0bnOWWWWWWWWWWWWWWWWWWWWWWWWqvESs:cLxfKW6yZk8/iZfMjYxnzonm9MaKcuwW
MD5:	877784A5F5808CEFA2B61E73BFCF8EAE
SHA1:	6A0E7EDA2734D7BBBA3CE38D37B347DF001B1DBF
SHA-256:	BE7F0632337BC381D4962125545A5CC3C1E84E2D03DBDB97AB3D79AD78B91B6D
SHA-512:	DABFFC928F7ED2A2D05003DAEF643806BD1CEC6B98E705F7415A82AFE7034F4E1E8A70C5AE69B094A948EEDAB4E8B76DCF72DF881DA092FE4AB76DA0EEFB8C3C
Malicious:	false
Reputation:	low
Preview:	......@@.... .(@..F... .... .(...n@..... .(....P..... .(....Y..(...@..... .....W.X..~S...W...X...X..X..V..p...}.....kQ.W*..S$..wK..k..k..k..m..m..p..q..q..r..~.....".....t..s'..^...\...^..._...._...`...a...b...e...M.....fF.^...sB...m...v...w...x...x...y...{...{.....%...#..."..."... .....v..._..xL...V...X...X...Y...Z...Z...\...`..}N...k#.....rO4.Y+...T...k...q...q...p...q...q...u...}...."...$... .....j...S...T...X...Z...Y...Z...[...Z...]..._..{O...o?.....

Chrome Cache Entry: 181

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded

Size (bytes):	1498
Entropy (8bit):	4.81759827491068
Encrypted:	false
SSDEEP:	24:UhvVovixQcvUvED/frfnQYRKYKvZiANncisDmZu7SECywEZS9Y6f:U7ZM8vbA3smgm89CywYkV
MD5:	11FE4E6509513DB245F1F97E37C5D3AB
SHA1:	05322C35B6BFAE84CE8C626BD7B1F8C4A6F15A6D
SHA-256:	78D437B40A85299F96ED9D02E35F23FD3D3EF63D844D8D2523A15516F7E1D09C
SHA-512:	E8A7C3B06C54B671FF6772D6A360DD0B4A65888B4DBD32AE04D14E4971343A71E1B4EC1E58BD45898744A1B0DF4EDE24141FF47E2C0393E18AACFC97E6F10D76
Malicious:	false
Reputation:	low
URL:	http://https://passwordreset.microsoftonline.com/css/ltrStyle.css?v=1342177280
Preview:	.paddingright { padding-right: 20px; }...paddingleft { padding-left: 20px; }...paddingright7 { padding-right: 7px; }...paddingleft7 { padding-left: 7px; }...paddingleft10 {padding-left: 10px; }...alignright { text-align: right; }...alignleft { text-align: left; }...leftalign {text-align: left; margin-left:0px;}.....borderRight {border-right: 1px solid black; padding: 0px;}.....userTypeRadioButtonMargin{margin-left: 10px; margin-top:50px;}...userVerificationInputLabel {text-align:left;padding-right: 10px;}...radioButtonMoreInformation { padding-left: 20px }.....header .logo{float:left; padding-left:30px;}.....HelpCallout td.PosRight{padding: 8px 0px 0px 0px; margin: 0px; vertical-align: top; font-size: 1px; border: none !important; background-color: transparent !important;}...HelpCallout td.PosRight > div{font-size: 1px; position: relative; left: 1px; border-bottom: none !important; border-right: none !important; border-left: none !important; width: 15px; background-color: transparent !

Chrome Cache Entry: 182

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (39257), with CRLF line terminators
Category:	downloaded
Size (bytes):	40326
Entropy (8bit):	5.245555585297941
Encrypted:	false
SSDEEP:	384:bvrc3TrJ1vMZCKZ4pLRy6DkfDLcbTzcXanT2rxb64aKQr1vySAwBaPUge6ydE:bTaYB4Hy7mTzcaTKStrwSAwBaPUTdE
MD5:	DA9DC1C32E89C02FC1E9EEB7E5AAB91E
SHA1:	3EFB110EFA6068CE6B586A67F87DA5125310BC30
SHA-256:	398CDF1B27EF247E5BC77805F266BB441E60355463FC3D1776F41AAE58B08CF1
SHA-512:	D4730EBC4CA62624B8300E292F27FD79D42A9277E409545DF7DC916189ED9DF13E46FAA37E3924B85A7C7EA8C76BF65A05ECA69B4029B550430536EC6DF8552A
Malicious:	false
Reputation:	low
URL:	http://https://passwordreset.microsoftonline.com/ScriptResource.axd?d=7GGcvh1NJlagbOi_gR4XkZFUXHZ6kkwYj4KCdjrP_PmqgAkIb6286tO0RccWuEC-dpg6M3SzH8t9YCYPpcvwZXML6uG08vZyuUp3J0XjZDc2Odz9uK2NsXnvb5iM0aTz5uxrTIe8O_FPp55HuG8IUeN9aQWR82KX7eWeYd_cb0dF5OGD__L1Mf20EcryXNVTGV0hK-Id9yFiTZZOygwfoD9KshXHIfuNPt6Dwhturxk1&t=74258c30
Preview:	//----------..// Copyright (C) Microsoft Corporation. All rights reserved...//----------..// MicrosoftAjaxWebForms.js..Type._registerScript("MicrosoftAjaxWebForms.js",["MicrosoftAjaxCore.js","MicrosoftAjaxSerialization.js","MicrosoftAjaxNetwork.js","MicrosoftAjaxComponentModel.js"]);Type.registerNamespace("Sys.WebForms");Sys.WebForms.BeginRequestEventArgs=function(c,b,a){Sys.WebForms.BeginRequestEventArgs.initializeBase(this);this._request=c;this._postBackElement=b;this._updatePanelsToUpdate=a};Sys.WebForms.BeginRequestEventArgs.prototype={get_postBackElement:function(){return this._postBackElement},get_request:function(){return this._request},get_updatePanelsToUpdate:function(){return this._updatePanelsToUpdate?Array.clone(this._updatePanelsToUpdate):[]}};Sys.WebForms.BeginRequestEventArgs.registerClass("Sys.WebForms.BeginRequestEventArgs",Sys.EventArgs);Sys.WebForms.EndRequestEventArgs=fun

Chrome Cache Entry: 183

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 60 x 60, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1561
Entropy (8bit):	7.762338770217686
Encrypted:	false
SSDEEP:	48:c/CeK/fE+XoVldlkPdTWbuf173xX964boBdlhLE:ntcx/lksbuf17f64borlK
MD5:	8DC34013E911C5F68FC2BCA0400CB06F
SHA1:	16BAFA91AF100D65C4945F04E0C6E1643B98CF00
SHA-256:	795029D360C3D16233FCE96F1BFF13C261535C0885FAE806CFF766F32D96BCEE
SHA-512:	83ACA42A30BFD629BC1E88D3ED154475E7949C1B154D19E6C9EF1DE825BA7967C0B6DA9EE79E7B420668242CCE5931DF344C97278A254F0A72C3D09EABED651
Malicious:	false
Reputation:	low
URL:	http://https://client.ppe.repmap.microsoft.com/Images/hipaudioplay.png?vv=100
Preview:	.PNG.....IHDR...<...<.....:..r....sBIT....|.d.....pHYs.....S.....tEXtCreation Time.05/06/16...o....tEXtSoftware.Adobe Fireworks CS6.....qIDATh..=l.E.....H..H*.|... ...&.D.).@....&...N....)_.E ...(.p...p(H...Ht.. ..0.....i.}s.....{`ss....;.....:...u..."....Az.r.%.9.|....wU.j...o....N4...~....g.u.=`.;..9.7.%....Ad#.....9....~7.....&.a.....`]x^D....&,"..kv.l..K.S+!.. ..#{.xm.;..%.+F<.\..#...bN...2...\.".I..U]..#.dWy$."r.2;Z...w)oD..H..u..M.'.k70.<4aG..`'~.....k31W.2!Ue.A"..j....X..C...dNUd.... .j.|c."..../..P.MXD.....C`>7Y.K...n.....U..#..^4. ...Uu...Q.);.`9q.53..n.@.....A6.E,6.-d; .....nl.>..."..N7..9\6.....p^a..4aG...3...gUu#..j...2.....f.....^.)...Udo'&..G.C.Z...L).....".t...pCD..n..a.....E....F...o.k.Y+b...[...gT..... ...]. ...V..m.!\..SCwh8w..J^.3N.....\.W.....3.....lP.Da.....-.....@_...i.....r..%..)E.Q...3..M..o.$...`..."....-/EHIDZ.q.MC.....D.Q..".. ..#.....1...p.x?dKP.=...{u\.

Chrome Cache Entry: 184	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	26951
Entropy (8bit):	4.514992390210281
Encrypted:	false
SSDEEP:	384:jMgviMjM4if38GmhXeC1QRwweTkBE9wbOY4Jf/JhRZ5h+73hNVt8oC4veONhLYVi:CLEiJSdo11vlYHqb5Klo8v
MD5:	B3D7A123BE5203A1A3F0F10233ED373F
SHA1:	F4C61F321D8F79A805B356C6EC94090C0D96215C
SHA-256:	EF9453F74B2617D43DCEF4242CF5845101FCFB57289C81BCEB20042B0023A192
SHA-512:	A01BFE8546E59C8AF83280A795B3F56DFA23D556B992813A4EB70089E80621686C7B51EE87B3109502667CAF1F95CBCA074BF607E543A0390BF6F8BB3ECD992E
Malicious:	false
Reputation:	low
URL:	http://https://passwordreset.microsoftonline.com/ScriptResource.axd?d=OQP9deB7nPNWTNnlbA3Oe7VYnAefc2EyWwA43KwE8yhC8e8iF5MPkyZjWvVvcL8kGhMPhWhQWFSvvC24miZnPZLzqFYmW79woKiFWo_G2e8TAeSM3oiKZjCQ_R2dMQOzil0PEOqwwbswY5sdhYFN_0-RJniS8fwWJU916l5F7idl-vbk2qoPqmMcdO8MDro4tpTcvyDMjJYEbFi3phG49w2&t=ffffffffa8ad04d3
Preview:	var Page_ValidationVer = "125";..var Page_IsValid = true;..var Page_BlockSubmit = false;..var Page_InvalidControlToBeFocused = null;..var Page_TextTypes = /^(text|password|file|search|tel|url|email|number|range|color|datetime|date|month|week|time|datetime-local)$/i;..function ValidatorUpdateDisplay(val) {.. if (typeof(val.display) == "string") {.. if (val.display == "None") {.. return;.. }.. if (val.display == "Dynamic") {.. val.style.display = val.isvalid ? "none" : "inline";.. return;.. }.. }.. if ((navigator.userAgent.indexOf("Mac") > -1) &&.. (navigator.userAgent.indexOf("MSIE") > -1)) {.. val.style.display = "inline";.. }.. val.style.visibility = val.isvalid ? "hidden" : "visible";..}..function ValidatorUpdateIsValid() {.. Page_IsValid = AllValidatorsValid(Page_Validators);..}..function AllValidatorsValid(validators) {.. if ((typeof(validators) != "undefined") && (validators != null)) {

Chrome Cache Entry: 185	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 16 x 25, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	405
Entropy (8bit):	6.927238031773719
Encrypted:	false
SSDEEP:	6:6v/lhPGtyR8R/Chm+jnDs9cCXz6fXlpvl+WOcy0f11VTaENo+7PfW3e37zt1afwp:6v/7SyG/HYfXJOvU1zTa8o+W8
MD5:	D4FFE61373F6AA32EEB8CA7CD41AB980
SHA1:	4925FAC4BC73EFB7C7BBC32B11C435ECF1D61674
SHA-256:	D5C54FFC6B8BD44D932BE8F37B1CD5B666205C7574F9D56EF68E56F83E08FFAD
SHA-512:	0F7EDE96F20BB3C053C246FFE1EF8CE739CEF7757FAAED031A365299B88664A046557C2C7FDB3BADED070BA4EBA1A14950D7E3A066B4976BF07142CEFA48BEEB
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....8.....sRGB.....gAMA.....a.....pHYs.....+.....tEXtSoftware.Adobe ImageReadyq.e<....IDAT8O...0...nf..y.,X4.g.I.h4..H.`.b.bA..f.n....%.=.iS.?N....^....A.(...~.i..m[.Qyz..iB..(...8...<G.....y..$.8....EQ.u]..I..(R.I...a...=..?t...CUU.....-..7.!..@.u0\..y.@..[a...p@.J.....e..>.Y..i..>A...+.,[. X9..z....B.4..+)..`n/..Q..>...y....e<....IEND.B`.

Chrome Cache Entry: 186	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 89 x 18, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1805
Entropy (8bit):	7.265265285391204
Encrypted:	false
SSDEEP:	24:oV1hpunQWwjx82lY2T32HEV8KJyJ3VAyKOGpxbAKJcyIXRP6VEBxX4pAE60KKAU9:4itNn2VMJ3R6breHDBBThFtYeD5B2
MD5:	BC89C1FBFBC227DC5A7ED9B2797E240D
SHA1:	8A9390297FDD0963C466CF2FD35D5B1F88A46B6A
SHA-256:	744A8CD0A4D15DFCF4A5D2E832FF556D950F8AF24D7B66104AB2EF4FE2605D9A
SHA-512:	C18F6B22F4AC5040E3FEBE8034AD3A3A3EF32CF3384BE6C3144B2EB04080F03111743D5B30AF3A1343AFD68A20AAE5972422C724107243D00CD9CF263DDC1007
Malicious:	false

Reputation:	low
Preview:	.PNG.....IHDR...Y.....0.r.....sRGB.....gAMA.....a.....tEXtSoftware.Adobe ImageReadyq.e<... iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpC ehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.0-c060 61.134777, 2010/02/12-17:32:00 "> <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/m m/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CS5 Windows" xmpMM:InstanceID="xmp.iid:BABFACAF90151 1E2BD4FDE5C526470CF" xmpMM:DocumentID="xmp.did:BABFACB0901511E2BD4FDE5C526470CF"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:BAB FACAD901511E2BD4FDE5C526470CF" stRef:documentID="xmp.did:BABFACAE901511E2BD4FDE5C526470CF"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xp acket end="r"?>..R....fIDATXG.mq[1.E.!...3&...P.....3..~L..q.O..t..{...v?..n.....b#.-.i..

Chrome Cache Entry: 187

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 720 x 405, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	237919
Entropy (8bit):	**7.9963496614328**
Encrypted:	**true**
SSDEEP:	6144:gL2xib7UwE0BfGqmRrAk0pFysvAxSHR++Kh44Hzckxq:jxi3N1mt0Xsl+B27
MD5:	8B91FDADC21BBE0468671EBB2688DC87
SHA1:	F9FEA146526696893D026932E1030C82108C28B5
SHA-256:	5E336553D4B87CB8CBA3013CF94AC3F454890D0173F40482715A40CBB6D0CA22
SHA-512:	40354E806AE3D20277228441D9AE22F6D89C098C7FF142DE864C17714261AD0363D0F429AF76A6C036C5EC75DD64F3CC13238A413CFF53DC419C435D8C8B813
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msftauthimages.net/dbd5a2dd-lfa6jvlreimgywhhs-c8kmaqnihskpfu3l8mv5xcc9i/logintenantbranding/0/illustration?ts=637441741242033826
Preview:	.PNG.....IHDR.....*.... .IDATx..[.$..%..Y=.C...?..F...&..e....Hx\|y.....p.!@.%q#.o.....n.Zk.Q....j.@...X.+.>.y.H$..-.....u...>.t.\<Z.~O.JH..R..D...LY...u.8...x}K.8m.m.% .k/..T..c..x!Y..D|..l..h*.D..t#.lG..W.v.E...@...cxN7.G..FN.F4*.u..N)...e.....S.@?h.kR5..%.w..t..TO.1c&i.Kz.chY~.x.....|V.....L....zA..FM.+.y.2.n+.]..3o..$/..."...rJ...7o=l..; .G.....Da..6....._.....]....H.....%3\|j.....+[....Tw..i.i..`3.\..K.@h]...&.4.2\|j...%'...NwOZ.J.ym.1.....d.%.!M...U..y.....)D.[.*.l.u...T.....j.....E.h.....;*o....g4...f4..w..Cf.....{.Oo.. <..g..;BJ\..]D.. .A.l...fF.....u.....&{..o..$c..c. .D.<..Ow..IW..K..B.yQb..^.....8._...[....";.;.n....F...g...}s.T..S...7.kwh.g...V\Y&S.1..Q..Qk..5..w.....Cv.8;l..y?....,)A.9....! ...n@..;...rk..7....U..\&.[..<..>..L.....F.h...B.\.....j.u..N.B^.daP.~.... ...s.9C!..G....2...,#z)..\...{.~Z....LR...``.aT:.9.bu..0|...PgO..)|9+.}F.f.7..a.....R..sa..(.[~..x.g=Ze

Chrome Cache Entry: 188

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 720 x 405, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	237919
Entropy (8bit):	**7.9963496614328**
Encrypted:	**true**
SSDEEP:	6144:gL2xib7UwE0BfGqmRrAk0pFysvAxSHR++Kh44Hzckxq:jxi3N1mt0Xsl+B27
MD5:	8B91FDADC21BBE0468671EBB2688DC87
SHA1:	F9FEA146526696893D026932E1030C82108C28B5
SHA-256:	5E336553D4B87CB8CBA3013CF94AC3F454890D0173F40482715A40CBB6D0CA22
SHA-512:	40354E806AE3D20277228441D9AE22F6D89C098C7FF142DE864C17714261AD0363D0F429AF76A6C036C5EC75DD64F3CC13238A413CFF53DC419C435D8C8B813
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....*.... .IDATx..[.$..%..Y=.C...?..F...&..e....Hx\|y.....p.!@.%q#.o.....n.Zk.Q....j.@...X.+.>.y.H$..-.....u...>.t.\<Z.~O.JH..R..D...LY...u.8...x}K.8m.m.% .k/..T..c..x!Y..D|..l..h*.D..t#.lG..W.v.E...@...cxN7.G..FN.F4*.u..N)...e.....S.@?h.kR5..%.w..t..TO.1c&i.Kz.chY~.x.....|V.....L....zA..FM.+.y.2.n+.]..3o..$/..."...rJ...7o=l..; .G.....Da..6....._.....]....H.....%3\|j.....+[....Tw..i.i..`3.\..K.@h]...&.4.2\|j...%'...NwOZ.J.ym.1.....d.%.!M...U..y.....)D.[.*.l.u...T.....j.....E.h.....;*o....g4...f4..w..Cf.....{.Oo.. <..g..;BJ\..]D.. .A.l...fF.....u.....&{..o..$c..c. .D.<..Ow..IW..K..B.yQb..^.....8._...[....";.;.n....F...g...}s.T..S...7.kwh.g...V\Y&S.1..Q..Qk..5..w.....Cv.8;l..y?....,)A.9....! ...n@..;...rk..7....U..\&.[..<..>..L.....F.h...B.\.....j.u..N.B^.daP.~.... ...s.9C!..G....2...,#z)..\...{.~Z....LR...``.aT:.9.bu..0|...PgO..)|9+.}F.f.7..a.....R..sa..(.[~..x.g=Ze

Chrome Cache Entry: 189

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1525
Entropy (8bit):	4.80220321270831
Encrypted:	false
SSDEEP:	24:jQB6rLbbhhye8jDjpfj/MALSj0eajoq0MgV05SkuVTgEbwe/sT5wiMa3sr6sHr3H:j8eLrynvlwIeyoJMluVEE0B7srH
MD5:	ACA0F1B02DC406E76DDC5F2BDEBEC6CE
SHA1:	594C930BE86B8843377565E349D2A10F1755A13A
SHA-256:	0446C6FD9AEB7DCD7CC089FA25323B1AE9AFA77B4CF8D4449F7D2D1B2467393A
SHA-512:	06887860F73D38799FFF8BF5B2972160B68C303EC904813861190E9A8A6477E4D300882994D661FDFC118C408625C537D8B28287DC9941D50302BD91C88ED98F
Malicious:	false

Reputation:	low
URL:	http://https://passwordreset.microsoftonline.com/js/Common.js
Preview:	.....function GetCookieValue(cookieName)..{.. if (document.cookie == undefined || document.cookie == "").. return "";.... var name = cookieName + "=";.. var cookieArray = document.cookie.split(';');.. for (var i = 0; i < cookieArray.length; i++).. {.. var clientCookie = cookieArray[i].trim();.. if (clientCookie.indexOf(name) == 0).. {.. return clientCookie.substring(name.length, clientCookie.length);.. }.. }.. return "";..}....function DeleteCookie(name)..{.. if (GetCookieValue(name).length > 0).. {.. document.cookie = name + "=" + ";expires=Thu, 01 Jan 2000 00:00:01 GMT";.. }..}....function GetUserSessionData(key) {.. var sessionStorage = window.sessionStorage;.. if (sessionStorage[key] == null) {.. return "";.. }.. return sessionStorage.getItem(key);..}....function SetUserSessionData(key, value) {.. var sessionStorage = window.sessionStorage;.. sessionStorage.setItem(key, val

Chrome Cache Entry: 190	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (64612)
Category:	downloaded
Size (bytes):	113657
Entropy (8bit):	5.491055924169325
Encrypted:	false
SSDEEP:	1536:VlqCwY8gIRPY0+r5qnWisnv9ILXtlTJCwggqdq/7XtvUN5bHo:EgDTMnWBaTJggqkDxUbzo
MD5:	B6783C7717E4042517138D9C9A48C867
SHA1:	7A7D6B0F36C2A3B557F1A75461630D433E5F4942
SHA-256:	4BE11C075187615ADAF493D54CB7B05556E76806AED2B3B082D72952D0025BE5
SHA-512:	2A322A8377784CBE543C978F32CB811388658F2E328B0024580D83DDE24AF0E131276AA76FEBED0B3AD1073ABCA8189AB9CD40BC4D36CFD93C0A1ECDAD63B05
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msftauth.net/shared/1.0/content/js/asyncchunk/convergedlogin_pstringcustomizationhelper_ea3e62a2bdfb2b2ee8c8.js
Preview:	/*!. * -- START OF THIRD PARTY NOTICE ---. * . * This file is based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise.. * . * json2.js (2016-05-01). * https://github.com/douglascrockford/JSON-js. * License: Public Domain. * . * Provided for Informational Purposes Only. * . * --- END OF THIRD PARTY NOTICE --. */.(window.webpackJsonp=window.webpackJsonp||[]).push([[37],{488:function(e,t,r

Chrome Cache Entry: 191	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 6 icons, -128x-128, 16 colors, 72x72, 16 colors
Category:	dropped
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsLsQZp:nfgyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD01
Malicious:	false
Reputation:	low
Preview:	..............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(....................(...................................."P.."""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333""""""""""""""""""""""""""""""

Chrome Cache Entry: 192	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	68
Entropy (8bit):	4.625316929997096
Encrypted:	false
SSDEEP:	3:tpSf4Ck8efFlK5ly:tak8efFlyly
MD5:	D1690731F22021E1466FBCD0DB6326EF
SHA1:	78F95BA0B7F82BBB7067000242DE860594ABD9C3

SHA-256:	490216DF4F089BB5C249BCF4034D0671254CA4236EC3ECA935AAC4B17E0FC7F3
SHA-512:	10B3CE812684D28DC72B74BA220E9A0DEE38550D49D25BB40B9EEB8764EE386E5F530D28A5E7C8E159B5C672D85D8649B102F3F04BD96092F9787ACACA4DBD F1
Malicious:	false
Reputation:	low
URL:	http://https://content-autofill.googleapis.com/v1/pages/ChVDaHJvbWUvMTE3LjAuNTkzOC4xMzISLAnYh4U85ulXExIFDURbFPwSBQ2L4FIoEgUNxK_d4xIFDW1rCkoSBQ2VKJT-?alt=proto
Preview:	CjEKCw1EWxT8GgQIZBgCCgcNi+BSKBoACgcNxK/d4xoACgcNbWsKShoACgcNlSiU/hoA

Chrome Cache Entry: 193	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	46376
Entropy (8bit):	4.760560792293901
Encrypted:	false
SSDEEP:	768:QgRN7ChZGd/5zEhQ49zXWV/eTSLtiMK7OQyOYZ:V1d/5edgVrlH
MD5:	DBFAC7887A157C9B73DC42927FC15B74
SHA1:	435FD188BF66F0207EEB298DD13228D17D36E4D1
SHA-256:	FC66E3943BC6EDC7B1F79D952D31DABCBA3BD576190DEEB9A7518CEE6B75C5A1
SHA-512:	C1918B35A03BD2110C2CB4EAD140BA342C54EE7BEE2C1E4B6582B56B86DA93AECDDA92DA626C7B15BDEBC067893ACD354919495551E71EE0C9D5993B43433 958
Malicious:	false
Reputation:	low
URL:	http://https://passwordreset.microsoftonline.com/js/Webtrends.js
Preview:	// WebTrends SmartSource Data Collector Tag..// Version: 8.6.2..// MS Version: 3.2.5..// Tag Builder Version: 3.0..// Created: 04/01/2011..function WebTrends() {.. var that = this;.. if (typeof (gDcsId) != "undefined" && gDcsId) this.dcsid = gDcsId;.. else this.dcsid = "not_a_valid_dcsid";.. if (typeof (gDomain) != "undefined" && gDomain) this.domain = gDomain;.. else this.domain = "m.webtrends.com";.. if (typeof (gTimeZone) != "undefined" && gTimeZone) this.timezone = gTimeZone;.. el se this.timezone = -8;.. if (typeof (gFpcDom) != "undefined" && gFpcDom) this.fpcdom = gFpcDom;.. else {.. if (/microsoft.com$/.test(window.location.hostname)) {.. this.fpcdom = ".microsoft.com";.. } else {.. this.fpcdom = window.location.hostname;.. }.. }.. if (typeof (gOffsite) != "undefined" && gOffsite).. if (gOffsite == true || gOffsite == "true") this.fpcdom = "";.. this.navigationtag = "div,table";.. if (typeof

Chrome Cache Entry: 194	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 22 x 22
Category:	downloaded
Size (bytes):	478
Entropy (8bit):	7.072122642964318
Encrypted:	false
SSDEEP:	12:d44xCq3nQQ5Q36sd0Tc/ET4Io9yjPy00EjNF8:d40CqXQQ5E69qEkI4Wy0lNF8
MD5:	309B41EE7A44BD51E5D1B52CCC620E5B
SHA1:	B162CE55DE01BF7C005F8CE4D4D7C32E7AEACA08
SHA-256:	F213507641FD02EC43981535823474ECFDE973D1B33A6CD385F1F0827FD4B528
SHA-512:	9279138126F8FEDD3AEF32BA4BCD78D3D26BBD4E7DE6F3B21014B96C34D7E69BC4C6471CC94772346CB6C7F9020EB5FE1A3A96686A5B250F5CCDEE54A0936 4D
Malicious:	false
Reputation:	low
URL:	http://https://passwordreset.microsoftonline.com/images/hip_text.gif
Preview:	GIF89a....;....333.....ZZY.....fff.....ssr.....MML.....@@@.....!....;,.....p.+.....9. P'..D.`.....t..pB\C.k..n...[..x7hRt..x7-}.92....}%p5.+..8..9552...n2...#.3//...3../33..."*..3+.../9..22....3....+./.9.2.....9.....3.....}(.).....5.....7.....`.....,"J....D>Dlh...F4D(..I..I ..@...!..0]B..d%..*w...;

Chrome Cache Entry: 195	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (45741)
Category:	downloaded
Size (bytes):	141517
Entropy (8bit):	5.431280072502083
Encrypted:	false
SSDEEP:	1536:5FZ5EDQbTPRUbx3jog/MhSJvRkmYWp0BSYmvIxdL/Bpns0Vgt2CTJm0wTxFojd9F:jEorg/MQNn3vIPzDk80ZjT0qcePgg
MD5:	458DE95432EF8D4FCA28BB532B18C314
SHA1:	2A35163C1225E25DF8427B5D877CFE43299BE502

SHA-256:	3332D913029F564F91B3EE85ABB4FA444D8DB0F97B346804088FA4B9DA643F66
SHA-512:	5869F579F209365B4455FD478FA433E7F8671DF403830098CC548F63306E1BF57E91806FB7AFF0835E9B97DFD7AE69332133798945B02569FAECBCE2D11C06B9
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msftauth.net/shared/1.0/content/js/BssoInterrupt_Core_RY3pVDLvjU_KKLtTKxjDFA2.js
Preview:	/*!. * ---------- START OF THIRD PARTY NOTICE ----------. * . * This file is based on or incorporates material from the project listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise.. * . * json2.js (2016-05-01). * https://github.com/douglascrockford/JSON-js. * License: Public Domain. * . * Provided for Informational Purposes Only. * . * ---------- END OF THIRD PARTY NOTICE ----------. */!function(e){function n(n){for(var t,r,i=n[0],a=n[1],s=0,u=[];s<i.length;s++)

Chrome Cache Entry: 196

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 89 x 18, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1805
Entropy (8bit):	7.265265285391204
Encrypted:	false
SSDEEP:	24:oV1hpunQWwjx82lY2T32HEV8KJyJ3VAyKOGpxbAKJcyIXRP6VEBxX4pAE60KKAU9:4itNn2VMJ3R6breHDBBThFtYeD5B2
MD5:	BC89C1FBFBC227DC5A7ED9B2797E240D
SHA1:	8A9390297FDD0963C466CF2FD35D5B1F88A46B6A
SHA-256:	744A8CD0A4D15DFCF4A5D2E832FF556D950F8AF24D7B66104AB2EF4FE2605D9A
SHA-512:	C18F6B22F4AC5040E3FEBE8034AD3A3A3EF32CF3384BE6C3144B2EB04080F03111743D5B30AF3A1343AFD68A20AAE5972422C724107243D00CD9CF263DDC1007
Malicious:	false
Reputation:	low
URL:	http://https://passwordreset.microsoftonline.com/images/header_microsoft.png
Preview:	.PNG.....IHDR...Y.....0.r.....sRGB.....gAMA.....a.....tEXtSoftware.Adobe ImageReadyq.e<... iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.0-c060 61.134777, 2010/02/12-17:32:00 "> <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 CS5 Windows" xmpMM:InstanceID="xmp.iid:BABFACAF901511E2BD4FDE5C526470CF" xmpMM:DocumentID="xmp.did:BABFACB0901511E2BD4FDE5C526470CF"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:BABFACAD901511E2BD4FDE5C526470CF" stRef:documentID="xmp.did:BABFACAE901511E2BD4FDE5C526470CF"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>..R....fIDATXG.mq[1.E.!...3&...P.....3..~L..q.O..t..{...v?..n.....b#.-.i..

Chrome Cache Entry: 197

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Unicode text, UTF-8 text, with very long lines (32097)
Category:	downloaded
Size (bytes):	55363
Entropy (8bit):	5.379785367870357
Encrypted:	false
SSDEEP:	1536:ABqF1tlfretkF7IKbVaqDRx3/ym+d/Px2g+0wtlQixnqTPRUbx3VDg/MvXI:ABrkF7IyJvym+d/Pog+0wtlQiUig/Mt
MD5:	BD317FFEFFE3D89877BF63931BD9372D
SHA1:	042DDBB953EFD7BDFF3D22AD97BCA0A81EB57149
SHA-256:	1EC2987C5CA4DC62E68F417FD75187C267E3ED438167546396CE913019F9FFFC
SHA-512:	831A77B3353CAD7F5D8CBDAA936A7A9468BAF9B94AEB8C60F5D763CC2C13C4EF3195771910446FE9265C0A230A924365CFE5B6F9AA86A06EA5C37262884CB8AF
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/ux.converged.login.strings-en.min_vtf__v_j2jh3v2otg9k3lq2.js
Preview:	!function(e){function o(n){if(i[n])return i[n].exports;var t=i[n]={exports:{},id:n,loaded:!1};return e[n].call(t.exports,t,t.exports,o),t.loaded=!0,t.exports}var i={};return o.m=e,o.c=i,o.p="",o(0)}([function(e,o,i){i(2);var n=i(1),t=i(5),r=i(6),a=r.StringsVariantId,s=r.AllowedIdentitiesType;n.registerSource("str",function(e,o){if(e.WF_STR_SignupLink_AriaLabel_Text="Create a Microsoft account",e.WF_STR_SignupLink_AriaLabel_Generic_Text="Create a new account",e.CT_STR_CookieBanner_Link_AriaLabel="Learn more about Microsoft's Cookie Policy",e.WF_STR_HeaderDefault_Title=o.iLoginStringsVariantId===a.CombinedSigninSignupV2WelcomeTitle?"Welcome":"Sign in",e.STR_Footer_IcpLicense_Text=".ICP.13015306.-10",o.oAppCobranding&&o.oAppCobranding.friendlyAppName){var i=o.fBreakBrandingSigninString?"to continue to {0}":"Continue to {0}";e.WF_STR_App_Title=t.format(i,o.oAppCobranding.friendlyAppName)}switch(o.oAppCobranding&&o.oAppCobranding.signinDescription&&(e.WF_STR_Default_Desc=o.oAppCobrand

Chrome Cache Entry: 198

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 22 x 22
Category:	dropped
Size (bytes):	478

Entropy (8bit):	7.072122642964318
Encrypted:	false
SSDEEP:	12:d44xCq3nQQ5Q36sd0Tc/ET4Io9yjPy00EjNF8:d40CqXQQ5E69qEkI4Wy0lNF8
MD5:	309B41EE7A44BD51E5D1B52CCC620E5B
SHA1:	B162CE55DE01BF7C005F8CE4D4D7C32E7AEACA08
SHA-256:	F213507641FD02EC43981535823474ECFDE973D1B33A6CD385F1F0827FD4B528
SHA-512:	9279138126F8FEDD3AEF32BA4BCD78D3D26BBD4E7DE6F3B21014B96C34D7E69BC4C6471CC94772346CB6C7F9020EB5FE1A3A96686A5B250F5CCDEE54A0936 4D
Malicious:	false
Reputation:	low
Preview:	GIF89a.....;....333.....ZZY.....fff.....ssr.....MML.....@@@.....!....;.,.....p.+.....9. P'..D.`.....t..pB\C.k..n...[..x7hRt..x7-}.92....}%p5.+..8..9552...n2...#.3//...3../33...'*..3+.../9..22....3....+./.9.2.....9.....3.....}(.).....5.....7.....`.....,"J....D>Dlh...F4D(..I..I ..@...!..0]B..d%..*w...;

Chrome Cache Entry: 199

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 24 x 24
Category:	downloaded
Size (bytes):	2463
Entropy (8bit):	6.994052150121201
Encrypted:	false
SSDEEP:	48:H0itvnLUG0J3nL8VO2ocia6Dk4MAbpGW4YBE/2p:HfNmT2QDnMAbsWTp
MD5:	93DE6FB07C1382459E473381DA5D0E7E
SHA1:	4E1208D482A7ABA8C86FDCF8E0E92C90BB8C8C8A
SHA-256:	E97FA0CFE4B0A7BB22E9713A67D4667DA064E674A944D607E78F0D3BF48E57A5
SHA-512:	B415DE10B55639DD5DFDD038FD490B675059122373659DD86AA00EBC7F6735FD22360264226F8675741FB76F3B3A16E9AB7FA907F489B377EF16E9222AA26E3B
Malicious:	false
Reputation:	low
URL:	http://https://passwordreset.microsoftonline.com/images/wait_animation.gif
Preview:	GIF89a.....!..NETSCAPE2.0.....!..XMP DataXMP<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.0-c060 61.134777, 2010/02/12-17:32:00 "> <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/" xm pMM:OriginalDocumentID="xmp.did:BCB95722648AE111A86BB806ED51E581" xmpMM:DocumentID="xmp.did:185F1A028B0511E19AA1A07B5BDC793D" xmpM M:InstanceID="xmp.iid:185F1A018B0511E19AA1A07B5BDC793D" xmp:CreatorTool="Adobe Photoshop CS5 Windows"> <xmpMM:DerivedFrom stRef:instanceID=" xmp.iid:D7EC7F987A8AE111A86BB806ED51E581" stRef:documentID="xmp.did:BCB95722648AE111A86BB806ED51E581"/> </rdf:Description> </rdf:RDF> </x:xm pmeta> <?xpacket end="r"?>.....

Chrome Cache Entry: 200

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 192 x 103, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	8360
Entropy (8bit):	7.923599325221617
Encrypted:	false
SSDEEP:	192:KTdWiPEkbEcxdpJTKabqLc73FEVhLmgez+S1vhXpj5AUqpVL:KdWiPEkEcfr32PLmge6ovhX95kL
MD5:	91821BD2E6B92C98235D686A1EED2143
SHA1:	196B7D9C770638AB60021063E2E49097B081B1B9
SHA-256:	381DCF4936A6D425D97D719E4E4C47A2A6D07A7933F16709AEC9AE383FBFC716
SHA-512:	50D6B7C2B1666BBB1379F289AD61B306BFD8C339244A5050BFFC8C02FE82BC3EF2D542927CF982F4F33E4C6B208D9FAA76E2D1FD1E89EEB66D5CC9541353F2 9
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....g.....V.MQ....sRGB.....gAMA.....a.....pHYs...t...t..f.x....tEXtSoftware.Adobe ImageReadyq.e<...&iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 7.1-c000 79.98d7942, 2022/03/21-11:40:59 "> <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.c om/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop 22.5 (Macintosh)" xmpMM:InstanceID="xmp. iid:4F012883FBAE11ECB5C18791D51607AC" xmpMM:DocumentID="xmp.did:4F012884FBAE11ECB5C18791D51607AC"> <xmpMM:DerivedFrom stRef:instan ceID="xmp.iid:4F012881FBAE11ECB5C18791D51607AC" stRef:documentID="xmp.did:4F012882FBAE11ECB5C18791D51607AC"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>...;....IDATx^..|T...O2K.IB....*....."P.Z.(...-.....E.O[..

Chrome Cache Entry: 201

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65447)
Category:	downloaded

Size (bytes):	81480
Entropy (8bit):	5.292219077408476
Encrypted:	false
SSDEEP:	1536:DjExXUqJnxDjoXEZxkMV4QYSt0zvDL6gP3h8cApwEIOzVTB/UjPazMdLiX4mF:DIh8GgP3hujzwbhd3Y
MD5:	83713513412973906E8AF09A0273990E
SHA1:	4C4BBCE9495EAA024FCE23D605A531ED45CF3D82
SHA-256:	601831BF3AF536E09A0B447B06785D00160C234C3073EE13B4DD19D6AAAFC68A
SHA-512:	1EAAC5DF3B4A39F47331CC930C0B4D2C2574FEC15156F141421DB1CF092C87452A02A285F071019B2759729A2431977B209A397D71B93A406BDB525C4BC13EB
Malicious:	false
Reputation:	low
URL:	http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-3.6.0.min.js
Preview:	/*! jQuery v3.6.0 | (c) OpenJS Foundation and other contributors | jquery.org/license */.!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.expo rts?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(C,e){"use strict";var t=[],r=Object.getPrototypeOf,s=t.slice,g=t.flat?function(e){return t.flat.call(e)}:function(e){return t.concat.apply([],e)},u= t.push,i=t.indexOf,n={},o=n.toString,v=n.hasOwnProperty,a=v.toString,l=a.call(Object),y={},m=function(e){return"function"==typeof e&&"number"!=typeof e.nodeType &&"function"!=typeof e.item},x=function(e){return null!=e&&e===e.window},E=C.document,c={type:!0,src:!0,nonce:!0,noModule:!0};function b(e,t,n){var r,i,o=(n=n|| E).createElement("script");if(o.text=e,t)for(r in c)(i=t[r]||t.getAttribute&&t.getAttribute(r))&&o.setAttribute(r,i);n.head.appendChild(o).parentNode.removeChild(o)}funct

Chrome Cache Entry: 202

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1378
Entropy (8bit):	4.316299265862323
Encrypted:	false
SSDEEP:	24:t4pb8m3NquUzOqnXmZcU4BC+CaAIA5cAEisx+fUu3fLkY:zoNLUzOeXfU4BJxA5fXUWx
MD5:	F83EBFF69A4A1685E4DC9650CDAB8886
SHA1:	FD21658884945B00157557AE06803DAA6A9F10C6
SHA-256:	7B1669DA90261CDB1483950BB480AD96875F84B09BC48D1055303CE94821BF64
SHA-512:	AA21A03AB84FA0129AFCED8A56E499757A6625C9B24A81EE08F5775B9B542F71BA67EAE817D633CB4E4533A8CF6A0DDA80BD7EE8A90E95AB3D39A77F88073F 23
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msftauth.net/shared/1.0/content/images/picker_account_aad_a8332c62695d74843a11daf39a74e552.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="48" height="48" viewBox="0 0 48 48"><defs><style>.a{fill:#e6e6e6;}.b{fill:#404040;}</style></defs><circle class="a" cx="24" cy="24" r="24"/><path class="b" d="M32.5,14A1.492,1.492,0,0,1,34,15.5V38.5A1.494,1.494,0,0,1,32.5,40h-17A1.494,1.494,0,0,1,14,38.5v-23A1.494,1.494,0, 0,1,15.5,14h4.873l-3-6h2.25l3,6h2.751l3-6h2.25l-3,6ZM32,16H23.623l1.266,2.546A1.13,1.13,0,0,1,25,19a1.009,1.009,0,0,1-1,1,1,1,1,0,0,1-.534-.149.974.974,0,0,1-.368- .4L21.375,16H16v22H32ZM20,26a3.92,3.92,0,0,1,.312-1.555,4.023,4.023,0,0,1,2.133-2.133,4.041,4.041,0,0,1,3.109,0,4.014,4.014,0,0,1,2.133,2.133A3.886,3.886,0,0,1 ,28,26a3.937,3.937,0,0,1-.288,1.485,3.987,3.987,0,0,1-.8,1.266A5.7,5.7,0,0,1,28.2,29.7a5.907,5.907,0,0,1,.968,1.251,6.388,6.388,0,0,1,.616,1.461A5.786,5.786,0,0 ,1,30,34H28a3.877,3.877,0,0,0-.312-1.554,4,4,0,0,0-2.133-2.133,4.011,4.011,0,0,0-3.109,0,4.023,4.023,0,0,0-2.133,2.133A3.912,3.912,0,0,0,20,33.995H18a5.786,5.78 6,0,0,1,.218-1.586,6.388,6.388,0,0,1,.61

Chrome Cache Entry: 203

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65329), with CRLF line terminators
Category:	downloaded
Size (bytes):	102801
Entropy (8bit):	5.336080509196147
Encrypted:	false
SSDEEP:	1536:MGLiogSomRYvoGtT+KHsVS0bT79DSsi46j/LPyR7kbE:MGLXGFKT79DSs6WCE
MD5:	C89EAA5B28DF1E17376BE71D71649173
SHA1:	2B34DF4C66BB57DE5A24A2EF0896271DFCA4F4CD
SHA-256:	66B804E7A96A87C11E1DD74EA04AC2285DF5AD9043F48046C3E5000114D39B1C
SHA-512:	B73D56304986CD587DA17BEBF21341B450D41861824102CC53885D863B118F6FDF2456B20791B9A7AE56DF91403F342550AF9E46F7401429FBA1D4A15A6BD3C0
Malicious:	false
Reputation:	low
URL:	http://https://passwordreset.microsoftonline.com/ScriptResource.axd?d=8m_SiUloDIADQm1m07iktYXf0pIre31vq34T5xPNqSSZviUhrOs_VUR3tiOw4GaoI-MvB_kJ0JIVWDZvGjT-RaAYJ7pLsTkHP4UOqxzlf3a4F_ERmwg3QCLiSa9rfNtIDFD-zZoCmgOQQ1o2-_uuK_OyFuPWlmRdlGxdqAscz1qv2js5qg9veVBGu6brm49phnQ18QIolbWRsRAijSW1Z9E6uSJ6EeaRH4aUxl0f-_w1&t=74258c30
Preview:	//----------..// Copyright (C) Microsoft Corporation. All rights reserved..//----------..// MicrosoftAjax.js..Fu ction.__typeName="Function";Function.__class=true;Function.createCallback=function(b,a){return function(){var e=arguments.length;if(e>0){var d=[];for(var c=0;c< e;c++)d[c]=arguments[c];d[e]=a;return b.apply(this,d)}return b.call(this,a)}};Function.createDelegate=function(a,b){return function(){return b.apply(a,arguments)}};Functi on.emptyFunction=Function.emptyMethod=function(){};Function.validateParameters=function(c,b,a){return Function._validateParams(c,b,a)};Function._validateParams= function(g,e,c){var a,d=e.length;c=c||typeof c==="undefined";a=Function._validateParameterCount(g,e,c);if(a){a.popStackFrame();return a}for(var b=0,i=g.length;b<i;b++) {var f=e[Math.min(b,d-1)],h=f.name;if(f.parameterArray)h+="["+(b-d+1)+"]";else if(!c&&b>=d)break;a=Function._validateParameter(g[b],f

Chrome Cache Entry: 204	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (64616)
Category:	downloaded
Size (bytes):	409596
Entropy (8bit):	5.460317664181365
Encrypted:	false
SSDEEP:	6144:IFR9WW8L65lcf6d/1GmpccqspdKmY0O9OnrYz:IF+W1GmpJDpkmpYz
MD5:	74F81077DDD865963051B0D007623E01
SHA1:	CCB91BA16783454A46DE7608C1DFD03DD49BC28B
SHA-256:	98C0872339E166FC98D211C46849DD6E739397F427E23B241CED88C5C126E2A9
SHA-512:	34948BA430E69B63B1479CE3A16820C3FE352D12BD83ED350F8CB4F93E51910765A364A5F3092672878B9AD75D31F73724AA1AEAAAEE173C6A72CEC8A3DB7D9F
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msftauth.net/shared/1.0/content/js/ConvergedLogin_PCore_T2EBBtMmyv072RjbQwNpoQ2.js
Preview:	/*!. * ---------- START OF THIRD PARTY NOTICE ----------. * . * This file is based on or incorporates material from the project listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise.. * . * json2.js (2016-05-01). * https://github.com/douglascrockford/JSON-js. * License: Public Domain. * . * Provided for Informational Purposes Only. * . * ---------- END OF THIRD PARTY NOTICE ----------. */!function(e){function n(n){for(var t,i,o=n[0],r=n[1],s=0,c=[];s<o.length;s++)

Chrome Cache Entry: 205	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 24 x 24
Category:	dropped
Size (bytes):	2463
Entropy (8bit):	6.994052150121201
Encrypted:	false
SSDEEP:	48:H0itvnLUG0J3nL8VO2ocia6Dk4MAbpGW4YBE/2p:HfNmT2QDnMAbsWTp
MD5:	93DE6FB07C1382459E473381DA5D0E7E
SHA1:	4E1208D482A7ABA8C86FDCF8E0E92C90BB8C8C8A
SHA-256:	E97FA0CFE4B0A7BB22E9713A67D4667DA064E674A944D607E78F0D3BF48E57A5
SHA-512:	B415DE10B55639DD5DFDD038FD490B675059122373659DD86AA00EBC7F6735FD22360264226F8675741FB76F3B3A16E9AB7FA907F489B377EF16E9222AA26E3B
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!..NETSCAPE2.0.....!..XMP DataXMP<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.0-c060 61.134777, 2010/02/12-17:32:00 "> <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:OriginalDocumentID="xmp.did:BCB95722648AE111A86BB806ED51E581" xmpMM:DocumentID="xmp.did:185F1A028B0511E19AA1A07B5BDC793D" xmpMM:InstanceID="xmp.iid:185F1A018B0511E19AA1A07B5BDC793D" xmp:CreatorTool="Adobe Photoshop CS5 Windows"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:D7EC7F987A8AE111A86BB806ED51E581" stRef:documentID="xmp.did:BCB95722648AE111A86BB806ED51E581"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.....

Chrome Cache Entry: 206	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 338 x 72, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4020
Entropy (8bit):	7.929907559552797
Encrypted:	false
SSDEEP:	96:1X+Yg6let+ZpBmQKEuhA/4oJqNoCkQV+CX8h:Fg69t+YfPhEBPnC+t
MD5:	36AFB641BECFAD75FED5F4E6E8C39268
SHA1:	2495652F017B7A06D796AFE9C4A06ECD54F9CCFE
SHA-256:	5C2192A3932CB78B431A1AC0F3F3D73414A31C63D5CB279F2687E58C72694200
SHA-512:	08C27020CF80A181B941EE144090FFBDD12ED34BA8CBEC037ACECE63F850FF8A69BE6DDB0EC24F7141C46F27779ED59AF84A55FB367C1B6F8893B444F44C5AF5
Malicious:	false
Reputation:	low

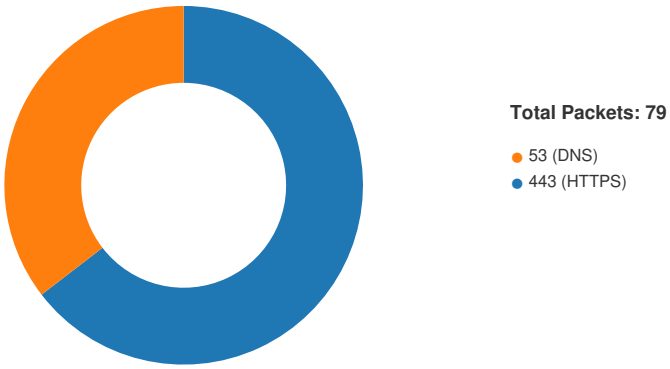
Preview:	.PNG.....IHDR...R...H.....}.....pHYs..!8..!8.E.1`....sRGB.....gAMA.....a....IIDATx...r....[ZZ..V.'0.....].....z....M..U.%.....C.....}...s...mIV.O5..... ...U.Hq@b.....Y..../)..hy.._S.....KzK...O\5EQ...(....B.(.....(J *...(...*....B.(.....(J *...(...*....B.(..H..EQ.C...V...7.//...~...?.....h4:.@TH.E....}.....k.v....L./.@TH...pGN.;.....'.(s...k.....4GTH...'O.~...g[..o.."....l..>.G...;..~...&.....d..u.^F.....M.h.....>.}>.....[.....E.b..?.u..{.B.....M._.iAh.>~.<*S...=.@`e..e....R...._ViA.E....R.@...@..vm.'Ei.v..\>QD..e..R.....;o.p{...../^d..TH;., F>..6...1?..E.p.}..J.p...XD.....7*.^b..../.w.....n0.+R.V).J.a..^.X.S..B(..W+++..W. ..e%"Z.[.{.....JQ.iG`....(5..e..`u.*.=.)J.....C.!.@..;$.i.F...W.[....#.....k.(J.z....`.dB..)..-H...R.H..O.#V..%.....W.4>.'..aJ9.2Q..+.R..id`.x..1.. .../.(J%..>2d.QJ..7.|.S`..10>..}.M#.....4.....<f}..OWO..m.;C[;u.|P!.....L...S.Egr.....3.k.....i.....O...

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 24, 2024 21:30:23.099047899 CEST	49675	443	192.168.2.4	173.222.162.32
May 24, 2024 21:30:32.160589933 CEST	49735	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:32.160686016 CEST	443	49735	13.107.136.10	192.168.2.4
May 24, 2024 21:30:32.160763025 CEST	49735	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:32.161025047 CEST	49736	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:32.161047935 CEST	443	49736	13.107.136.10	192.168.2.4
May 24, 2024 21:30:32.161092043 CEST	49736	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:32.161266088 CEST	49735	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:32.161300898 CEST	443	49735	13.107.136.10	192.168.2.4
May 24, 2024 21:30:32.161575079 CEST	49736	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:32.161585093 CEST	443	49736	13.107.136.10	192.168.2.4
May 24, 2024 21:30:32.707879066 CEST	49675	443	192.168.2.4	173.222.162.32
May 24, 2024 21:30:32.750893116 CEST	443	49736	13.107.136.10	192.168.2.4
May 24, 2024 21:30:32.751144886 CEST	49736	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:32.751154900 CEST	443	49736	13.107.136.10	192.168.2.4
May 24, 2024 21:30:32.752808094 CEST	443	49736	13.107.136.10	192.168.2.4
May 24, 2024 21:30:32.752870083 CEST	49736	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:32.754017115 CEST	49736	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:32.754100084 CEST	443	49736	13.107.136.10	192.168.2.4
May 24, 2024 21:30:32.755575895 CEST	49736	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:32.755584002 CEST	443	49736	13.107.136.10	192.168.2.4
May 24, 2024 21:30:32.764748096 CEST	443	49735	13.107.136.10	192.168.2.4
May 24, 2024 21:30:32.765003920 CEST	49735	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:32.765064001 CEST	443	49735	13.107.136.10	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 24, 2024 21:30:32.768676996 CEST	443	49735	13.107.136.10	192.168.2.4
May 24, 2024 21:30:32.768775940 CEST	49735	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:32.769171953 CEST	49735	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:32.769387007 CEST	443	49735	13.107.136.10	192.168.2.4
May 24, 2024 21:30:32.802382946 CEST	49736	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:32.817720890 CEST	49735	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:32.817779064 CEST	443	49735	13.107.136.10	192.168.2.4
May 24, 2024 21:30:32.865020037 CEST	49735	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:32.929435968 CEST	443	49736	13.107.136.10	192.168.2.4
May 24, 2024 21:30:32.929683924 CEST	443	49736	13.107.136.10	192.168.2.4
May 24, 2024 21:30:32.929755926 CEST	49736	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:32.930094957 CEST	49736	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:32.930104971 CEST	443	49736	13.107.136.10	192.168.2.4
May 24, 2024 21:30:32.933001041 CEST	49735	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:32.974572897 CEST	443	49735	13.107.136.10	192.168.2.4
May 24, 2024 21:30:33.140707016 CEST	443	49735	13.107.136.10	192.168.2.4
May 24, 2024 21:30:33.140924931 CEST	443	49735	13.107.136.10	192.168.2.4
May 24, 2024 21:30:33.141139030 CEST	49735	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:33.173181057 CEST	49735	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:33.173240900 CEST	443	49735	13.107.136.10	192.168.2.4
May 24, 2024 21:30:33.246963978 CEST	49739	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:33.246989965 CEST	443	49739	13.107.136.10	192.168.2.4
May 24, 2024 21:30:33.247066021 CEST	49739	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:33.247265100 CEST	49739	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:33.247277021 CEST	443	49739	13.107.136.10	192.168.2.4
May 24, 2024 21:30:33.861534119 CEST	443	49739	13.107.136.10	192.168.2.4
May 24, 2024 21:30:33.861903906 CEST	49739	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:33.861912966 CEST	443	49739	13.107.136.10	192.168.2.4
May 24, 2024 21:30:33.863086939 CEST	443	49739	13.107.136.10	192.168.2.4
May 24, 2024 21:30:33.864434004 CEST	49739	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:33.864559889 CEST	49739	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:33.864563942 CEST	443	49739	13.107.136.10	192.168.2.4
May 24, 2024 21:30:33.864645004 CEST	443	49739	13.107.136.10	192.168.2.4
May 24, 2024 21:30:33.898834944 CEST	49740	443	192.168.2.4	142.250.185.164
May 24, 2024 21:30:33.898868084 CEST	443	49740	142.250.185.164	192.168.2.4
May 24, 2024 21:30:33.898926973 CEST	49740	443	192.168.2.4	142.250.185.164
May 24, 2024 21:30:33.899497986 CEST	49740	443	192.168.2.4	142.250.185.164
May 24, 2024 21:30:33.899517059 CEST	443	49740	142.250.185.164	192.168.2.4
May 24, 2024 21:30:33.909840107 CEST	49739	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:34.135027885 CEST	443	49739	13.107.136.10	192.168.2.4
May 24, 2024 21:30:34.135077953 CEST	443	49739	13.107.136.10	192.168.2.4
May 24, 2024 21:30:34.135116100 CEST	49739	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:34.135118008 CEST	443	49739	13.107.136.10	192.168.2.4
May 24, 2024 21:30:34.135147095 CEST	443	49739	13.107.136.10	192.168.2.4
May 24, 2024 21:30:34.135185003 CEST	49739	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:34.135231972 CEST	443	49739	13.107.136.10	192.168.2.4
May 24, 2024 21:30:34.135363102 CEST	443	49739	13.107.136.10	192.168.2.4
May 24, 2024 21:30:34.135406017 CEST	49739	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:34.138186932 CEST	49739	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:34.138200045 CEST	443	49739	13.107.136.10	192.168.2.4
May 24, 2024 21:30:34.138206959 CEST	49739	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:34.138240099 CEST	49739	443	192.168.2.4	13.107.136.10
May 24, 2024 21:30:34.607604027 CEST	443	49740	142.250.185.164	192.168.2.4
May 24, 2024 21:30:34.609261990 CEST	49740	443	192.168.2.4	142.250.185.164
May 24, 2024 21:30:34.609292030 CEST	443	49740	142.250.185.164	192.168.2.4
May 24, 2024 21:30:34.610943079 CEST	443	49740	142.250.185.164	192.168.2.4
May 24, 2024 21:30:34.611083984 CEST	49740	443	192.168.2.4	142.250.185.164
May 24, 2024 21:30:34.663474083 CEST	49742	443	192.168.2.4	95.101.200.226
May 24, 2024 21:30:34.663491964 CEST	443	49742	95.101.200.226	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 24, 2024 21:30:34.663542032 CEST	49742	443	192.168.2.4	95.101.200.226
May 24, 2024 21:30:34.665685892 CEST	49742	443	192.168.2.4	95.101.200.226
May 24, 2024 21:30:34.665698051 CEST	443	49742	95.101.200.226	192.168.2.4
May 24, 2024 21:30:34.726686001 CEST	49740	443	192.168.2.4	142.250.185.164
May 24, 2024 21:30:34.727154970 CEST	443	49740	142.250.185.164	192.168.2.4
May 24, 2024 21:30:34.773276091 CEST	49740	443	192.168.2.4	142.250.185.164
May 24, 2024 21:30:34.773303986 CEST	443	49740	142.250.185.164	192.168.2.4
May 24, 2024 21:30:34.816221952 CEST	49740	443	192.168.2.4	142.250.185.164
May 24, 2024 21:30:35.387727976 CEST	443	49742	95.101.200.226	192.168.2.4
May 24, 2024 21:30:35.388247013 CEST	49742	443	192.168.2.4	95.101.200.226
May 24, 2024 21:30:35.392162085 CEST	49742	443	192.168.2.4	95.101.200.226
May 24, 2024 21:30:35.392169952 CEST	443	49742	95.101.200.226	192.168.2.4
May 24, 2024 21:30:35.392613888 CEST	443	49742	95.101.200.226	192.168.2.4
May 24, 2024 21:30:35.442442894 CEST	49742	443	192.168.2.4	95.101.200.226
May 24, 2024 21:30:35.481395960 CEST	49742	443	192.168.2.4	95.101.200.226
May 24, 2024 21:30:35.526503086 CEST	443	49742	95.101.200.226	192.168.2.4
May 24, 2024 21:30:35.671492100 CEST	443	49742	95.101.200.226	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 24, 2024 21:30:30.950541973 CEST	53	63729	1.1.1.1	192.168.2.4
May 24, 2024 21:30:30.950571060 CEST	53	63003	1.1.1.1	192.168.2.4
May 24, 2024 21:30:32.064557076 CEST	55808	53	192.168.2.4	1.1.1.1
May 24, 2024 21:30:32.064557076 CEST	58135	53	192.168.2.4	1.1.1.1
May 24, 2024 21:30:32.115868092 CEST	53	51609	1.1.1.1	192.168.2.4
May 24, 2024 21:30:33.883532047 CEST	49798	53	192.168.2.4	1.1.1.1
May 24, 2024 21:30:33.883984089 CEST	65092	53	192.168.2.4	1.1.1.1
May 24, 2024 21:30:33.891159058 CEST	53	49798	1.1.1.1	192.168.2.4
May 24, 2024 21:30:33.898248911 CEST	53	65092	1.1.1.1	192.168.2.4
May 24, 2024 21:30:34.140301943 CEST	58374	53	192.168.2.4	1.1.1.1
May 24, 2024 21:30:34.140985012 CEST	64554	53	192.168.2.4	1.1.1.1
May 24, 2024 21:30:36.026046038 CEST	59559	53	192.168.2.4	1.1.1.1
May 24, 2024 21:30:36.026171923 CEST	50454	53	192.168.2.4	1.1.1.1
May 24, 2024 21:30:36.041126966 CEST	53	59559	1.1.1.1	192.168.2.4
May 24, 2024 21:30:36.060033083 CEST	53	50454	1.1.1.1	192.168.2.4
May 24, 2024 21:30:39.176538944 CEST	63723	53	192.168.2.4	1.1.1.1
May 24, 2024 21:30:39.176636934 CEST	53637	53	192.168.2.4	1.1.1.1
May 24, 2024 21:30:47.145828009 CEST	60423	53	192.168.2.4	1.1.1.1
May 24, 2024 21:30:47.145936966 CEST	53449	53	192.168.2.4	1.1.1.1
May 24, 2024 21:30:47.188340902 CEST	55248	53	192.168.2.4	1.1.1.1
May 24, 2024 21:30:47.188599110 CEST	50479	53	192.168.2.4	1.1.1.1
May 24, 2024 21:30:47.198256016 CEST	53	60423	1.1.1.1	192.168.2.4
May 24, 2024 21:30:47.198291063 CEST	53	53449	1.1.1.1	192.168.2.4
May 24, 2024 21:30:48.791728973 CEST	51573	53	192.168.2.4	1.1.1.1
May 24, 2024 21:30:48.791728973 CEST	51462	53	192.168.2.4	1.1.1.1
May 24, 2024 21:30:48.839123011 CEST	64031	53	192.168.2.4	1.1.1.1
May 24, 2024 21:30:48.839353085 CEST	63551	53	192.168.2.4	1.1.1.1
May 24, 2024 21:30:48.852921009 CEST	53	64031	1.1.1.1	192.168.2.4
May 24, 2024 21:30:48.857666016 CEST	53	63551	1.1.1.1	192.168.2.4
May 24, 2024 21:30:49.176671028 CEST	53	61977	1.1.1.1	192.168.2.4
May 24, 2024 21:30:50.018194914 CEST	56740	53	192.168.2.4	1.1.1.1
May 24, 2024 21:30:50.018240929 CEST	64574	53	192.168.2.4	1.1.1.1
May 24, 2024 21:30:51.136069059 CEST	53	57770	1.1.1.1	192.168.2.4
May 24, 2024 21:30:52.291439056 CEST	138	138	192.168.2.4	192.168.2.255
May 24, 2024 21:31:05.435729980 CEST	65360	53	192.168.2.4	1.1.1.1
May 24, 2024 21:31:05.436083078 CEST	59319	53	192.168.2.4	1.1.1.1
May 24, 2024 21:31:06.746892929 CEST	52918	53	192.168.2.4	1.1.1.1
May 24, 2024 21:31:06.747090101 CEST	62055	53	192.168.2.4	1.1.1.1

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 24, 2024 21:31:08.267663956 CEST	53	65428	1.1.1.1	192.168.2.4
May 24, 2024 21:31:10.563368082 CEST	55458	53	192.168.2.4	1.1.1.1
May 24, 2024 21:31:10.563580990 CEST	50418	53	192.168.2.4	1.1.1.1
May 24, 2024 21:31:12.367348909 CEST	53	58428	1.1.1.1	192.168.2.4
May 24, 2024 21:31:29.329332113 CEST	53	62782	1.1.1.1	192.168.2.4
May 24, 2024 21:31:31.724355936 CEST	53	58210	1.1.1.1	192.168.2.4
May 24, 2024 21:31:40.307410955 CEST	51067	53	192.168.2.4	1.1.1.1
May 24, 2024 21:31:40.307657003 CEST	58842	53	192.168.2.4	1.1.1.1

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 24, 2024 21:30:33.898418903 CEST	192.168.2.4	1.1.1.1	c1fd	(Port unreachable)	Destination Unreachable
May 24, 2024 21:30:36.060110092 CEST	192.168.2.4	1.1.1.1	c243	(Port unreachable)	Destination Unreachable
May 24, 2024 21:31:05.535742998 CEST	192.168.2.4	1.1.1.1	c2c3	(Port unreachable)	Destination Unreachable
May 24, 2024 21:31:06.778287888 CEST	192.168.2.4	1.1.1.1	c25f	(Port unreachable)	Destination Unreachable
May 24, 2024 21:31:10.839221001 CEST	192.168.2.4	1.1.1.1	c2c0	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 24, 2024 21:30:32.064557076 CEST	192.168.2.4	1.1.1.1	0xa0d9	Standard query (0)	jmawireless-my.sharepoint.com	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:32.064557076 CEST	192.168.2.4	1.1.1.1	0x6f5a	Standard query (0)	jmawireless-my.sharepoint.com	65	IN (0x0001)	false
May 24, 2024 21:30:33.883532047 CEST	192.168.2.4	1.1.1.1	0x2274	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:33.883984089 CEST	192.168.2.4	1.1.1.1	0x85fe	Standard query (0)	www.google.com	65	IN (0x0001)	false
May 24, 2024 21:30:34.140301943 CEST	192.168.2.4	1.1.1.1	0x1ee1	Standard query (0)	login.microsoftonline.com	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:34.140985012 CEST	192.168.2.4	1.1.1.1	0x1d54	Standard query (0)	login.microsoftonline.com	65	IN (0x0001)	false
May 24, 2024 21:30:36.026046038 CEST	192.168.2.4	1.1.1.1	0xbbaf	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:36.026171923 CEST	192.168.2.4	1.1.1.1	0x631a	Standard query (0)	aadcdn.msftauth.net	65	IN (0x0001)	false
May 24, 2024 21:30:39.176538944 CEST	192.168.2.4	1.1.1.1	0x7251	Standard query (0)	identity.nel.measure.office.net	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:39.176636934 CEST	192.168.2.4	1.1.1.1	0x59ed	Standard query (0)	identity.nel.measure.office.net	65	IN (0x0001)	false
May 24, 2024 21:30:47.145828009 CEST	192.168.2.4	1.1.1.1	0xb682	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:47.145936966 CEST	192.168.2.4	1.1.1.1	0x3c76	Standard query (0)	aadcdn.msftauth.net	65	IN (0x0001)	false
May 24, 2024 21:30:47.188340902 CEST	192.168.2.4	1.1.1.1	0x8b3	Standard query (0)	login.microsoftonline.com	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:47.188599110 CEST	192.168.2.4	1.1.1.1	0x5281	Standard query (0)	login.microsoftonline.com	65	IN (0x0001)	false
May 24, 2024 21:30:48.791728973 CEST	192.168.2.4	1.1.1.1	0x1334	Standard query (0)	aadcdn.msftauthimages.net	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:48.791728973 CEST	192.168.2.4	1.1.1.1	0x5823	Standard query (0)	aadcdn.msftauthimages.net	65	IN (0x0001)	false
May 24, 2024 21:30:48.839123011 CEST	192.168.2.4	1.1.1.1	0x581d	Standard query (0)	autologon.microsoftazuread-sso.com	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:48.839353085 CEST	192.168.2.4	1.1.1.1	0x9bae	Standard query (0)	autologon.microsoftazuread-sso.com	65	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 24, 2024 21:30:50.018194914 CEST	192.168.2.4	1.1.1.1	0x7cff	Standard query (0)	aadcdn.msftauthimages.net	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:50.018240929 CEST	192.168.2.4	1.1.1.1	0x88c7	Standard query (0)	aadcdn.msftauthimages.net	65	IN (0x0001)	false
May 24, 2024 21:31:05.435729980 CEST	192.168.2.4	1.1.1.1	0xa5d3	Standard query (0)	passwordreset.microsoftonline.com	A (IP address)	IN (0x0001)	false
May 24, 2024 21:31:05.436083078 CEST	192.168.2.4	1.1.1.1	0x1b0f	Standard query (0)	passwordreset.microsoftonline.com	65	IN (0x0001)	false
May 24, 2024 21:31:06.746892929 CEST	192.168.2.4	1.1.1.1	0xa18b	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)	false
May 24, 2024 21:31:06.747090101 CEST	192.168.2.4	1.1.1.1	0xa3a7	Standard query (0)	ajax.aspnetcdn.com	65	IN (0x0001)	false
May 24, 2024 21:31:10.563368082 CEST	192.168.2.4	1.1.1.1	0x9925	Standard query (0)	passwordreset.microsoftonline.com	A (IP address)	IN (0x0001)	false
May 24, 2024 21:31:10.563580990 CEST	192.168.2.4	1.1.1.1	0x962a	Standard query (0)	passwordreset.microsoftonline.com	65	IN (0x0001)	false
May 24, 2024 21:31:40.307410955 CEST	192.168.2.4	1.1.1.1	0x72f6	Standard query (0)	identity.nel.measure.office.net	A (IP address)	IN (0x0001)	false
May 24, 2024 21:31:40.307657003 CEST	192.168.2.4	1.1.1.1	0xbe2d	Standard query (0)	identity.nel.measure.office.net	65	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 24, 2024 21:30:32.148082018 CEST	1.1.1.1	192.168.2.4	0x6f5a	No error (0)	jmawireless-my.sharepoint.com	jmawireless.sharepoint.com		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:32.148082018 CEST	1.1.1.1	192.168.2.4	0x6f5a	No error (0)	jmawireless.sharepoint.com	4501-ipv4v6e.clump.dprodmgd105.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:32.148082018 CEST	1.1.1.1	192.168.2.4	0x6f5a	No error (0)	4501-ipv4v6e.clump.dprodmgd105.aa-rt.sharepoint.com	192203-ipv4v6e.farm.dprodmgd105.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:32.148082018 CEST	1.1.1.1	192.168.2.4	0x6f5a	No error (0)	192203-ipv4v6e.farm.dprodmgd105.aa-rt.sharepoint.com	192203-ipv4v6e.farm.dprodmgd105.sharepointonline.com.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:32.159972906 CEST	1.1.1.1	192.168.2.4	0xa0d9	No error (0)	jmawireless-my.sharepoint.com	jmawireless.sharepoint.com		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:32.159972906 CEST	1.1.1.1	192.168.2.4	0xa0d9	No error (0)	jmawireless.sharepoint.com	4501-ipv4v6e.clump.dprodmgd105.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:32.159972906 CEST	1.1.1.1	192.168.2.4	0xa0d9	No error (0)	4501-ipv4v6e.clump.dprodmgd105.aa-rt.sharepoint.com	192203-ipv4v6e.farm.dprodmgd105.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:32.159972906 CEST	1.1.1.1	192.168.2.4	0xa0d9	No error (0)	192203-ipv4v6e.farm.dprodmgd105.aa-rt.sharepoint.com	192203-ipv4v6e.farm.dprodmgd105.sharepointonline.com.akadns.net		CNAME (Canonical name)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 24, 2024 21:30:32.159972906 CEST	1.1.1.1	192.168.2.4	0xa0d9	No error (0)	192203-ipv4v6.farm.dprodmgd105.aa-rt.sharepoint.com.dual-spo-0005.spo-msedge.net	dual-spo-0005.spo-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:32.159972906 CEST	1.1.1.1	192.168.2.4	0xa0d9	No error (0)	dual-spo-0005.spo-msedge.net		13.107.136.10	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:32.159972906 CEST	1.1.1.1	192.168.2.4	0xa0d9	No error (0)	dual-spo-0005.spo-msedge.net		13.107.138.10	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:33.891159058 CEST	1.1.1.1	192.168.2.4	0x2274	No error (0)	www.google.com		142.250.185.164	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:33.898248911 CEST	1.1.1.1	192.168.2.4	0x85fe	No error (0)	www.google.com			65	IN (0x0001)	false
May 24, 2024 21:30:34.231857061 CEST	1.1.1.1	192.168.2.4	0x1ee1	No error (0)	login.microsoftonline.com	login.mso.msidentity.com		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:34.231889963 CEST	1.1.1.1	192.168.2.4	0x1d54	No error (0)	login.microsoftonline.com	login.mso.msidentity.com		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:36.041126966 CEST	1.1.1.1	192.168.2.4	0xbbaf	No error (0)	aadcdn.msftauth.net	cs1100.wpc.omegacdn.net		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:36.041126966 CEST	1.1.1.1	192.168.2.4	0xbbaf	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:36.060033083 CEST	1.1.1.1	192.168.2.4	0x631a	No error (0)	aadcdn.msftauth.net	cs1100.wpc.omegacdn.net		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:39.203919888 CEST	1.1.1.1	192.168.2.4	0x7251	No error (0)	identity.nel.measure.office.net	nel.measure.office.net.edgesuite.net		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:39.203924894 CEST	1.1.1.1	192.168.2.4	0x59ed	No error (0)	identity.nel.measure.office.net	nel.measure.office.net.edgesuite.net		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:39.596025944 CEST	1.1.1.1	192.168.2.4	0x3b93	No error (0)	shed.dual-low.part-0039.t-0009.t-msedge.net	azurefd-t-fb-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:39.596025944 CEST	1.1.1.1	192.168.2.4	0x3b93	No error (0)	dual.part-0039.t-0009.fb-t-msedge.net	part-0039.t-0009.fb-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:39.596025944 CEST	1.1.1.1	192.168.2.4	0x3b93	No error (0)	part-0039.t-0009.fb-t-msedge.net		13.107.226.67	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:39.596025944 CEST	1.1.1.1	192.168.2.4	0x3b93	No error (0)	part-0039.t-0009.fb-t-msedge.net		13.107.253.67	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:46.709011078 CEST	1.1.1.1	192.168.2.4	0x501d	No error (0)	fp2e7a.wpc.2be4.phicdn.net	fp2e7a.wpc.phicdn.net		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:46.709011078 CEST	1.1.1.1	192.168.2.4	0x501d	No error (0)	fp2e7a.wpc.phicdn.net		192.229.221.95	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:47.198256016 CEST	1.1.1.1	192.168.2.4	0xb682	No error (0)	aadcdn.msftauth.net	cs1100.wpc.omegacdn.net		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:47.198256016 CEST	1.1.1.1	192.168.2.4	0xb682	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:47.198291063 CEST	1.1.1.1	192.168.2.4	0x3c76	No error (0)	aadcdn.msftauth.net	cs1100.wpc.omegacdn.net		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:47.209801912 CEST	1.1.1.1	192.168.2.4	0x8b3	No error (0)	login.microsoftonline.com	login.mso.msidentity.com		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:47.209831953 CEST	1.1.1.1	192.168.2.4	0x5281	No error (0)	login.microsoftonline.com	login.mso.msidentity.com		CNAME (Canonical name)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 24, 2024 21:30:48.801630020 CEST	1.1.1.1	192.168.2.4	0x1334	No error (0)	aadcdn.msftauthimages.net	aadcdn-msft.azureedge.net		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:48.801630020 CEST	1.1.1.1	192.168.2.4	0x1334	No error (0)	shed.dual-low.part-0032.t-0009.t-msedge.net	part-0032.t-0009.t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:48.801630020 CEST	1.1.1.1	192.168.2.4	0x1334	No error (0)	part-0032.t-0009.t-msedge.net		13.107.213.60	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:48.801630020 CEST	1.1.1.1	192.168.2.4	0x1334	No error (0)	part-0032.t-0009.t-msedge.net		13.107.246.60	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:48.806442022 CEST	1.1.1.1	192.168.2.4	0x5823	No error (0)	aadcdn.msftauthimages.net	aadcdn-msft.azureedge.net		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:48.852921009 CEST	1.1.1.1	192.168.2.4	0x581d	No error (0)	autologon.microsoftazuread-sso.com		40.126.32.138	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:48.852921009 CEST	1.1.1.1	192.168.2.4	0x581d	No error (0)	autologon.microsoftazuread-sso.com		40.126.32.76	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:48.852921009 CEST	1.1.1.1	192.168.2.4	0x581d	No error (0)	autologon.microsoftazuread-sso.com		40.126.32.140	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:48.852921009 CEST	1.1.1.1	192.168.2.4	0x581d	No error (0)	autologon.microsoftazuread-sso.com		40.126.32.68	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:48.852921009 CEST	1.1.1.1	192.168.2.4	0x581d	No error (0)	autologon.microsoftazuread-sso.com		20.190.160.22	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:48.852921009 CEST	1.1.1.1	192.168.2.4	0x581d	No error (0)	autologon.microsoftazuread-sso.com		40.126.32.134	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:48.852921009 CEST	1.1.1.1	192.168.2.4	0x581d	No error (0)	autologon.microsoftazuread-sso.com		20.190.160.14	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:48.852921009 CEST	1.1.1.1	192.168.2.4	0x581d	No error (0)	autologon.microsoftazuread-sso.com		40.126.32.72	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:50.063606977 CEST	1.1.1.1	192.168.2.4	0x7cff	No error (0)	aadcdn.msftauthimages.net	aadcdn-msft.azureedge.net		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:50.063606977 CEST	1.1.1.1	192.168.2.4	0x7cff	No error (0)	shed.dual-low.part-0039.t-0009.t-msedge.net	part-0039.t-0009.t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:30:50.063606977 CEST	1.1.1.1	192.168.2.4	0x7cff	No error (0)	part-0039.t-0009.t-msedge.net		13.107.246.67	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:50.063606977 CEST	1.1.1.1	192.168.2.4	0x7cff	No error (0)	part-0039.t-0009.t-msedge.net		13.107.213.67	A (IP address)	IN (0x0001)	false
May 24, 2024 21:30:50.075333118 CEST	1.1.1.1	192.168.2.4	0x88c7	No error (0)	aadcdn.msftauthimages.net	aadcdn-msft.azureedge.net		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:31:00.102899075 CEST	1.1.1.1	192.168.2.4	0xafa	No error (0)	fp2e7a.wpc.2be4.phicdn.net	fp2e7a.wpc.phicdn.net		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:31:00.102899075 CEST	1.1.1.1	192.168.2.4	0xafa	No error (0)	fp2e7a.wpc.phicdn.net		192.229.221.95	A (IP address)	IN (0x0001)	false
May 24, 2024 21:31:05.445131063 CEST	1.1.1.1	192.168.2.4	0xa5d3	No error (0)	passwordreset.microsoftonline.com	passwordreset.mso.msidentity.com		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:31:05.535536051 CEST	1.1.1.1	192.168.2.4	0x1b0f	No error (0)	passwordreset.microsoftonline.com	passwordreset.mso.msidentity.com		CNAME (Canonical name)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 24, 2024 21:31:06.757723093 CEST	1.1.1.1	192.168.2.4	0xa18b	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:31:06.778193951 CEST	1.1.1.1	192.168.2.4	0xa3a7	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:31:10.594994068 CEST	1.1.1.1	192.168.2.4	0x9925	No error (0)	passwordreset.microsoftonline.com	passwordreset.mso.msidentity.com		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:31:10.839139938 CEST	1.1.1.1	192.168.2.4	0x962a	No error (0)	passwordreset.microsoftonline.com	passwordreset.mso.msidentity.com		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:31:40.328933954 CEST	1.1.1.1	192.168.2.4	0x72f6	No error (0)	identity.nel.measure.office.net	nel.measure.office.net.edgesuite.net		CNAME (Canonical name)	IN (0x0001)	false
May 24, 2024 21:31:40.328946114 CEST	1.1.1.1	192.168.2.4	0xbe2d	No error (0)	identity.nel.measure.office.net	nel.measure.office.net.edgesuite.net		CNAME (Canonical name)	IN (0x0001)	false

HTTP Request Dependency Graph

- jmawireless-my.sharepoint.com
- fs.microsoft.com
- https:
  - aadcdn.msftauth.net
  - aadcdn.msauth.net
  - aadcdn.msftauthimages.net

Statistics

Behavior

Click to jump to process

System Behavior

All data are 0.

Disassembly

No disassembly